附錄

附錄一 美國電子化政府法

PUBLIC LAW 107–347—DEC. 17 2002 116 STAT. 2899

Public Law 107–347

107th Congress

An Act

To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ‘‘E-Government Act of 2002’’.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

Sec. 2. Findings and purposes.

TITLE I—OFFICE OF MANAGEMENT AND BUDGET ELECTRONIC GOVERNMENT SERVICES

Sec. 101. Management and promotion of electronic government services.

Sec. 102. Conforming amendments.

TITLE II—FEDERAL MANAGEMENT AND PROMOTION OF ELECTRONIC

GOVERNMENT SERVICES

Sec. 201. Definitions.

Sec. 202. Federal agency responsibilities.

Sec. 203. Compatibility of executive agency methods for use and acceptance of electronic signatures.

Sec. 204. Federal Internet portal.

Sec. 205. Federal courts.

Sec. 206. Regulatory agencies.

Sec. 207. Accessibility, usability, and preservation of government information.

Sec. 208. Privacy provisions.

Sec. 209. Federal information technology workforce development.

Sec. 210. Share-in-savings initiatives.

Sec. 211. Authorization for acquisition of information technology by State and local governments through Federal supply schedules.

Sec. 212. Integrated reporting study and pilot projects.

Sec. 213. Community technology centers.

Sec. 214. Enhancing crisis management through advanced information technology.

Sec. 215. Disparities in access to the Internet.

Sec. 216. Common protocols for geographic information systems.

TITLE III—INFORMATION SECURITY

Sec. 301. Information security.

Sec. 302. Management of information technology.

Sec. 303. National Institute of Standards and Technology.

Sec. 304. Information Security and Privacy Advisory Board.

Sec. 305. Technical and conforming amendments.

TITLE IV—AUTHORIZATION OF APPROPRIATIONS AND EFFECTIVE DATES

Sec. 401. Authorization of appropriations.

44 USC 101 note.

E-Government

Act of 2002.

Dec. 17, 2002

[H.R. 2458]

116 STAT. 2900 PUBLIC LAW 107–347—DEC. 17 2002

Sec. 402. Effective dates.

TITLE V—CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY

Sec. 501. Short title.

Sec. 502. Definitions.

Sec. 503. Coordination and oversight of policies.

Sec. 504. Effect on other laws.

Subtitle A—Confidential Information Protection

Sec. 511. Findings and purposes.

Sec. 512. Limitations on use and disclosure of data and information.

Sec. 513. Fines and penalties.

Subtitle B—Statistical Efficiency

Sec. 521. Findings and purposes.

Sec. 522. Designation of statistical agencies.

Sec. 523. Responsibilities of designated statistical agencies.

Sec. 524. Sharing of business data among designated statistical agencies.

Sec. 525. Limitations on use of business data provided by designated statistical agencies.

Sec. 526. Conforming amendments.

SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS.—Congress finds the following:

(1) The use of computers and the Internet is rapidly transforming societal interactions and the relationships among citizens,

private businesses, and the Government.
(2) The Federal Government has had uneven success in applying advances in information technology to enhance governmental functions and services, achieve more efficient performance, increase access to Government information, and increase citizen participation in Government.
(3) Most Internet-based services of the Federal Government are developed and presented separately, according to the jurisdictional boundaries of an individual department or agency, rather than being integrated cooperatively according to function or topic.
(4) Internet-based Government services involving interagency cooperation are especially difficult to develop and promote, in part because of a lack of sufficient funding mechanisms to support such interagency cooperation.
(5) Electronic Government has its impact through improved Government performance and outcomes within and across agencies.
(6) Electronic Government is a critical element in the management of Government, to be implemented as part of a management framework that also addresses finance, procurement, human capital, and other challenges to improve the performance of Government.
(7) To take full advantage of the improved Government performance that can be achieved through the use of Internetbased technology requires strong leadership, better organization, improved interagency collaboration, and more focused oversight of agency compliance with statutes related to information resource management.
(b) PURPOSES.—The purposes of this Act are the following:
(1) To provide effective leadership of Federal Government

efforts to develop and promote electronic Government services and processes by establishing an Administrator of a new Office of Electronic Government within the Office of Management and Budget.

44 USC 3601 note.

(2) To promote use of the Internet and other information technologies to provide increased opportunities for citizen participation in Government.

(3) To promote interagency collaboration in providing electronic Government services, where this collaboration would improve the service to citizens by integrating related functions, and in the use of internal electronic Government processes, where this collaboration would improve the efficiency and effectiveness of the processes.

(4) To improve the ability of the Government to achieve agency missions and program performance goals.

(5) To promote the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services.

(6) To reduce costs and burdens for businesses and other Government entities.

(7) To promote better informed decisionmaking by policy makers.

(8) To promote access to high quality Government information and services across multiple channels.

(9) To make the Federal Government more transparent

and accountable.

(10) To transform agency operations by utilizing, where appropriate, best practices from public and private sector organizations.

(11) To provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws.

TITLE I—OFFICE OF MANAGEMENT AND BUDGET ELECTRONIC GOVERNMENT SERVICES

SEC. 101. MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES.

(a) IN GENERAL.—Title 44, United States Code, is amended by inserting after chapter 35 the following:

‘‘CHAPTER 36—MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

‘‘Sec.

‘‘3601. Definitions.

‘‘3602. Office of Electronic Government.

‘‘3603. Chief Information Officers Council.

‘‘3604. E-Government Fund.

‘‘3605. Program to encourage innovative solutions to enhance electronic Government services and processes.

‘‘3606. E-Government report.

‘‘§ 3601. Definitions

‘‘In this chapter, the definitions under section 3502 shall apply, and the term—

‘‘(1) ‘Administrator’ means the Administrator of the Office of Electronic Government established under section 3602;

‘‘(2) ‘Council’ means the Chief Information Officers Council established under section 3603;

‘‘(3) ‘electronic Government’ means the use by the Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to—

‘‘(A) enhance the access to and delivery of Government information and services to the public, other agencies, and other Government entities; or

‘‘(B) bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation;

‘‘(4) ‘enterprise architecture’—

‘‘(A) means—

‘‘(i) a strategic information asset base, which defines the mission;

‘‘(ii) the information necessary to perform the mission;

‘‘(iii) the technologies necessary to perform the mission; and

‘‘(iv) the transitional processes for implementing new technologies in response to changing mission needs; and

‘‘(B) includes—

‘‘(i) a baseline architecture;

‘‘(ii) a target architecture; and

‘‘(iii) a sequencing plan;

‘‘(5) ‘Fund’ means the E-Government Fund established

under section 3604;

''(6) 'interoperability' means the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner;

''(7) 'integrated service delivery' means the provision of Internet-based Federal Government information or services integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction; and

''(8) 'tribal government' means—

''(A) the governing body of any Indian tribe, band, nation, or other organized group or community located in the continental United States (excluding the State of Alaska) that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians, and

''(B) any Alaska Native regional or village corporation established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.).

''§ 3602. Office of Electronic Government

''(a) There is established in the Office of Management and Budget an Office of Electronic Government.

''(b) There shall be at the head of the Office an Administrator who shall be appointed by the President.

''(c) The Administrator shall assist the Director in carrying out—

''(1) all functions under this chapter;

President.

Establishment.

Government

organization.

‘‘(2) all of the functions assigned to the Director under title II of the E-Government Act of 2002; and

‘‘(3) other electronic government initiatives, consistent with other statutes.

‘‘(d) The Administrator shall assist the Director and the Deputy Director for Management and work with the Administrator of the Office of Information and Regulatory Affairs in setting strategic direction for implementing electronic Government, under relevant statutes, including—

‘‘(1) chapter 35;

‘‘(2) subtitle III of title 40, United States Code;

‘‘(3) section 552a of title 5 (commonly referred to as the ‘Privacy Act’);

‘‘(4) the Government Paperwork Elimination Act (44 U.S.C. 3504 note); and

‘‘(5) the Federal Information Security Management Act of 2002.

‘‘(e) The Administrator shall work with the Administrator of the Office of Information and Regulatory Affairs and with other offices within the Office of Management and Budget to oversee implementation of electronic Government under this chapter, chapter 35, the E-Government Act of 2002, and other relevant statutes, in a manner consistent with law, relating to—

‘‘(1) capital planning and investment control for information technology;

‘‘(2) the development of enterprise architectures;

‘‘(3) information security;
‘‘(4) privacy;
‘‘(5) access to, dissemination of, and preservation of Government information;
‘‘(6) accessibility of information technology for persons with disabilities; and
‘‘(7) other areas of electronic Government.
‘‘(f) Subject to requirements of this chapter, the Administrator shall assist the Director by performing electronic Government functions as follows:
‘‘(1) Advise the Director on the resources required to develop and effectively administer electronic Government initiatives.
‘‘(2) Recommend to the Director changes relating to Governmentwide strategies and priorities for electronic Government.
‘‘(3) Provide overall leadership and direction to the executive branch on electronic Government.
‘‘(4) Promote innovative uses of information technology by agencies, particularly initiatives involving multiagency collaboration, through support of pilot projects, research, experimentation, and the use of innovative technologies.
‘‘(5) Oversee the distribution of funds from, and ensure appropriate administration and coordination of, the E-Government Fund established under section 3604.
‘‘(6) Coordinate with the Administrator of General Services regarding programs undertaken by the General Services Administration to promote electronic government and the efficient use of information technologies by agencies.

‘‘(7) Lead the activities of the Chief Information Officers Council established under section 3603 on behalf of the Deputy Director for Management, who shall chair the council.

‘‘(8) Assist the Director in establishing policies which shall set the framework for information technology standards for the Federal Government developed by the National Institute of Standards and Technology and promulgated by the Secretary of Commerce under section 11331 of title 40, taking into account, if appropriate, recommendations of the Chief Information Officers Council, experts, and interested parties from the private and nonprofit sectors and State, local, and tribal governments, and maximizing the use of commercial standards as appropriate, including the following:

‘‘(A) Standards and guidelines for interconnectivity and interoperability as described under section 3504.

‘‘(B) Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guidelines for categorizing Federal Government electronic information to enable efficient use of technologies, such as through the use of extensible markup language.

‘‘(C) Standards and guidelines for Federal Government computer system efficiency and security.

‘‘(9) Sponsor ongoing dialogue that—

‘‘(A) shall be conducted among Federal, State, local, and tribal government leaders on electronic Government in the executive, legislative, and judicial branches, as well as leaders in the private and nonprofit sectors, to encourage collaboration and enhance understanding of best practices and innovative approaches in acquiring, using, and managing information resources;

‘‘(B) is intended to improve the performance of governments in collaborating on the use of information technology to improve the delivery of Government information and services; and

‘‘(C) may include—

‘‘(i) development of innovative models—

‘‘(I) for electronic Government management and Government information technology contracts; and

‘‘(II) that may be developed through focused discussions or using separately sponsored research;

‘‘(ii) identification of opportunities for public-private collaboration in using Internet-based technology to increase the efficiency of Government-to-business transactions;

‘‘(iii) identification of mechanisms for providing incentives to program managers and other Government employees to develop and implement innovative uses of information technologies; and

‘‘(iv) identification of opportunities for public, private, and intergovernmental collaboration in addressing the disparities in access to the Internet and information technology.

‘‘(10) Sponsor activities to engage the general public in the development and implementation of policies and programs, particularly activities aimed at fulfilling the goal of using the most effective citizen-centered strategies and those activities

which engage multiple agencies providing similar or related information and services.

‘‘(11) Oversee the work of the General Services Administration and other agencies in developing the integrated Internetbased system under section 204 of the E-Government Act of 2002.

‘‘(12) Coordinate with the Administrator for Federal Procurement Policy to ensure effective implementation of electronic procurement initiatives.

‘‘(13) Assist Federal agencies, including the General Services Administration, the Department of Justice, and the United States Access Board in—

‘‘(A) implementing accessibility standards under section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d); and

‘‘(B) ensuring compliance with those standards through the budget review process and other means.

‘‘(14) Oversee the development of enterprise architectures within and across agencies.

‘‘(15) Assist the Director and the Deputy Director for Management in overseeing agency efforts to ensure that electronic Government activities incorporate adequate, risk-based, and cost-effective security compatible with business processes.

‘‘(16) Administer the Office of Electronic Government established under this section.

‘‘(17) Assist the Director in preparing the E-Government report established under section 3606.

‘‘(g) The Director shall ensure that the Office of Management and Budget, including the Office of Electronic Government, the Office of Information and Regulatory Affairs, and other relevant

offices, have adequate staff and resources to properly fulfill all functions under the E-Government Act of 2002.

''§ 3603. Chief Information Officers Council

''(a) There is established in the executive branch a Chief Information Officers Council.

''(b) The members of the Council shall be as follows:

''(1) The Deputy Director for Management of the Office of Management and Budget, who shall act as chairperson of the Council.

''(2) The Administrator of the Office of Electronic Government.

''(3) The Administrator of the Office of Information and Regulatory Affairs.

''(4) The chief information officer of each agency described under section 901(b) of title 31.

''(5) The chief information officer of the Central Intelligence Agency.

''(6) The chief information officer of the Department of the Army, the Department of the Navy, and the Department of the Air Force, if chief information officers have been designated for such departments under section 3506(a)(2)(B).

''(7) Any other officer or employee of the United States designated by the chairperson.

''(c)(1) The Administrator of the Office of Electronic Government shall lead the activities of the Council on behalf of the Deputy Director for Management.

Establishment.

''(2)(A) The Vice Chairman of the Council shall be selected

by the Council from among its members.

''(B) The Vice Chairman shall serve a 1-year term, and may serve multiple terms.

''(3) The Administrator of General Services shall provide administrative and other support for the Council.

''(d) The Council is designated the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of Federal Government information resources.

''(e) In performing its duties, the Council shall consult regularly with representatives of State, local, and tribal governments.

''(f) The Council shall perform functions that include the following:

''(1) Develop recommendations for the Director on Government information resources management policies and requirements.

''(2) Share experiences, ideas, best practices, and innovative approaches related to information resources management.

''(3) Assist the Administrator in the identification, development, and coordination of multiagency projects and other innovative initiatives to improve Government performance through the use of information technology.

''(4) Promote the development and use of common performance measures for agency information resources management under this chapter and title II of the E-Government Act of 2002.

''(5) Work as appropriate with the National Institute of Standards and Technology and the Administrator to develop recommendations on information technology standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated under section 11331 of title 40, and maximize the use of commercial

standards as appropriate, including the following:
‘‘(A) Standards and guidelines for interconnectivity and interoperability as described under section 3504.
‘‘(B) Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guidelines for categorizing Federal Government electronic information to enable efficient use of technologies, such as through the use of extensible markup language.
‘‘(C) Standards and guidelines for Federal Government computer system efficiency and security.
‘‘(6) Work with the Office of Personnel Management to assess and address the hiring, training, classification, and professional development needs of the Government related to information resources management.
‘‘(7) Work with the Archivist of the United States to assess how the Federal Records Act can be addressed effectively by Federal information resources management activities.

‘‘§ 3604. E-Government Fund

‘‘(a)(1) There is established in the Treasury of the United States the E-Government Fund.
‘‘(2) The Fund shall be administered by the Administrator of the General Services Administration to support projects approved by the Director, assisted by the Administrator of the Office of

Electronic Government, that enable the Federal Government to expand its ability, through the development and implementation of innovative uses of the Internet or other electronic methods, to conduct activities electronically.

‘‘(3) Projects under this subsection may include efforts to—
‘‘(A) make Federal Government information and services more readily available to members of the public (including individuals, businesses, grantees, and State and local governments);
‘‘(B) make it easier for the public to apply for benefits, receive services, pursue business opportunities, submit information, and otherwise conduct transactions with the Federal Government; and
‘‘(C) enable Federal agencies to take advantage of information technology in sharing information and conducting transactions with each other and with State and local governments.
‘‘(b)(1) The Administrator shall—
‘‘(A) establish procedures for accepting and reviewing proposals for funding;
‘‘(B) consult with interagency councils, including the Chief Information Officers Council, the Chief Financial Officers Council, and other interagency management councils, in establishing procedures and reviewing proposals; and
‘‘(C) assist the Director in coordinating resources that agencies receive from the Fund with other resources available to agencies for similar purposes.
‘‘(2) When reviewing proposals and managing the Fund, the Administrator shall observe and incorporate the following procedures:
‘‘(A) A project requiring substantial involvement or funding from an agency shall be approved by a senior official with agencywide authority on behalf of the head of the agency, who shall report directly to the head of the agency.
‘‘(B) Projects shall adhere to fundamental capital planning and investment control processes.
‘‘(C) Agencies shall identify in their proposals resource

commitments from the agencies involved and how these resources would be coordinated with support from the Fund, and include plans for potential continuation of projects after all funds made available from the Fund are expended.

''(D) After considering the recommendations of the interagency councils, the Director, assisted by the Administrator, shall have final authority to determine which of the candidate projects shall be funded from the Fund.

''(E) Agencies shall assess the results of funded projects.

''(c) In determining which proposals to recommend for funding, the Administrator—

''(1) shall consider criteria that include whether a proposal—

''(A) identifies the group to be served, including citizens, businesses, the Federal Government, or other governments;

''(B) indicates what service or information the project will provide that meets needs of groups identified under subparagraph (A);

''(C) ensures proper security and protects privacy;

Procedures.

''(D) is interagency in scope, including projects implemented by a primary or single agency that—

''(i) could confer benefits on multiple agencies; and

''(ii) have the support of other agencies; and

''(E) has performance objectives that tie to agency missions and strategic goals, and interim results that relate to the objectives; and

‘‘(2) may also rank proposals based on criteria that include whether a proposal—

‘‘(A) has Governmentwide application or implications;

‘‘(B) has demonstrated support by the public to be served;

‘‘(C) integrates Federal with State, local, or tribal approaches to service delivery;

‘‘(D) identifies resource commitments from nongovernmental sectors;

‘‘(E) identifies resource commitments from the agencies involved;

‘‘(F) uses web-based technologies to achieve objectives;

‘‘(G) identifies records management and records access strategies;

‘‘(H) supports more effective citizen participation in and interaction with agency activities that further progress toward a more citizen-centered Government;

‘‘(I) directly delivers Government information and services to the public or provides the infrastructure for delivery;

‘‘(J) supports integrated service delivery;

‘‘(K) describes how business processes across agencies will reflect appropriate transformation simultaneous to technology implementation; and

‘‘(L) is new or innovative and does not supplant existing funding streams within agencies.

‘‘(d) The Fund may be used to fund the integrated Internetbased system under section 204 of the E-Government Act of 2002.

‘‘(e) None of the funds provided from the Fund may be transferred to any agency until 15 days after the Administrator of the General Services Administration has submitted to the Committees

on Appropriations of the Senate and the House of Representatives, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, and the appropriate authorizing committees of the Senate and the House of Representatives, a notification and description of how the funds are to be allocated and how the expenditure will further the purposes of this chapter.

''(f)(1) The Director shall report annually to Congress on the operation of the Fund, through the report established under section 3606.

''(2) The report under paragraph (1) shall describe—

''(A) all projects which the Director has approved for funding from the Fund; and

''(B) the results that have been achieved to date for these funded projects.

''(g)(1) There are authorized to be appropriated to the Fund—

''(A) $45,000,000 for fiscal year 2003;

''(B) $50,000,000 for fiscal year 2004;

''(C) $100,000,000 for fiscal year 2005;

''(D) $150,000,000 for fiscal year 2006; and

Reports.

Notification.

''(E) such sums as are necessary for fiscal year 2007.

''(2) Funds appropriated under this subsection shall remain available until expended.

''§ 3605. Program to encourage innovative solutions to enhance electronic Government services and

processes

‘‘(a) ESTABLISHMENT OF PROGRAM.—The Administrator shall establish and promote a Governmentwide program to encourage contractor innovation and excellence in facilitating the development and enhancement of electronic Government services and processes.

‘‘(b) ISSUANCE OF ANNOUNCEMENTS SEEKING INNOVATIVE SOLUTIONS.—Under the program, the Administrator, in consultation with the Council and the Administrator for Federal Procurement Policy, shall issue announcements seeking unique and innovative solutions to facilitate the development and enhancement of electronic Government services and processes.

‘‘(c) MULTIAGENCY TECHNICAL ASSISTANCE TEAM.—(1) The Administrator, in consultation with the Council and the Administrator for Federal Procurement Policy, shall convene a multiagency technical assistance team to assist in screening proposals submitted to the Administrator to provide unique and innovative solutions to facilitate the development and enhancement of electronic Government services and processes. The team shall be composed of employees of the agencies represented on the Council who have expertise in scientific and technical disciplines that would facilitate the assessment of the feasibility of the proposals.

‘‘(2) The technical assistance team shall—

‘‘(A) assess the feasibility, scientific and technical merits, and estimated cost of each proposal; and

‘‘(B) submit each proposal, and the assessment of the proposal, to the Administrator.

‘‘(3) The technical assistance team shall not consider or evaluate proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

‘‘(4) After receiving proposals and assessments from the technical

assistance team, the Administrator shall consider recommending appropriate proposals for funding under the E-Government Fund established under section 3604 or, if appropriate, forward the proposal and the assessment of it to the executive agency whose mission most coincides with the subject matter of the proposal.

''§ 3606. E-Government report

''(a) Not later than March 1 of each year, the Director shall submit an E-Government status report to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives.

''(b) The report under subsection (a) shall contain—

''(1) a summary of the information reported by agencies under section 202(f) of the E-Government Act of 2002;

''(2) the information required to be reported by section 3604(f); and

''(3) a description of compliance by the Federal Government with other goals and provisions of the E-Government Act of 2002.''.

Deadline.

116 STAT. 2910 PUBLIC LAW 107–347—DEC. 17 2002

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of chapters for title 44, United States Code, is amended by inserting after the item relating to chapter 35 the following:

''36. Management and Promotion of Electronic Government Services 3601''.

SEC. 102. CONFORMING AMENDMENTS.

(a) ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGIES.—

(1) IN GENERAL.—Chapter 3 of title 40, United States Code, is amended by inserting after section 304 the following new

section:

‘‘§ 305. Electronic Government and information technologies

‘‘The Administrator of General Services shall consult with the Administrator of the Office of Electronic Government on programs undertaken by the General Services Administration to promote electronic Government and the efficient use of information technologies by Federal agencies.’’.

(2) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 3 of such title is amended by inserting after the item relating to section 304 the following:

‘‘305. Electronic Government and information technologies.’’.

(b) MODIFICATION OF DEPUTY DIRECTOR FOR MANAGEMENT FUNCTIONS.—Section 503(b) of title 31, United States Code, is amended—

(1) by redesignating paragraphs (5), (6), (7), (8), and (9), as paragraphs (6), (7), (8), (9), and (10), respectively; and

(2) by inserting after paragraph (4) the following:

‘‘(5) Chair the Chief Information Officers Council established under section 3603 of title 44.’’.

(c) OFFICE OF ELECTRONIC GOVERNMENT.—

(1) IN GENERAL.—Chapter 5 of title 31, United States Code, is amended by inserting after section 506 the following:

‘‘§ 507. Office of Electronic Government

‘‘The Office of Electronic Government, established under section 3602 of title 44, is an office in the Office of Management and Budget.’’.

(2) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 5 of title 31, United States Code, is amended by inserting after the item relating to section 506 the following:

‘‘507. Office of Electronic Government.’’.

TITLE II—FEDERAL MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

SEC. 201. DEFINITIONS.

Except as otherwise provided, in this title the definitions under sections 3502 and 3601 of title 44, United States Code, shall apply.

44 USC 3501 note.

PUBLIC LAW 107–347—DEC. 17 2002 116 STAT. 2911

SEC. 202. FEDERAL AGENCY RESPONSIBILITIES.

(a) IN GENERAL.—The head of each agency shall be responsible for—

(1) complying with the requirements of this Act (including the amendments made by this Act), the related information resource management policies and guidance established by the Director of the Office of Management and Budget, and the related information technology standards promulgated by the Secretary of Commerce;

(2) ensuring that the information resource management policies and guidance established under this Act by the Director, and the related information technology standards promulgated by the Secretary of Commerce are communicated promptly and effectively to all relevant officials within their agency; and

(3) supporting the efforts of the Director and the Administrator of the General Services Administration to develop, maintain, and promote an integrated Internet-based system of delivering

Federal Government information and services to the
public under section 204.
(b) PERFORMANCE INTEGRATION.—
(1) Agencies shall develop performance measures that demonstrate
how electronic government enables progress toward
agency objectives, strategic goals, and statutory mandates.
(2) In measuring performance under this section, agencies
shall rely on existing data collections to the extent practicable.
(3) Areas of performance measurement that agencies should
consider include—
(A) customer service;
(B) agency productivity; and
(C) adoption of innovative information technology,
including the appropriate use of commercial best practices.
(4) Agencies shall link their performance goals, as appropriate,
to key groups, including citizens, businesses, and other
governments, and to internal Federal Government operations.
(5) As appropriate, agencies shall work collectively in
linking their performance goals to groups identified under paragraph
(4) and shall use information technology in delivering
Government information and services to those groups.
(c) AVOIDING DIMINISHED ACCESS.—When promulgating policies
and implementing programs regarding the provision of Government
information and services over the Internet, agency heads shall
consider the impact on persons without access to the Internet,
and shall, to the extent practicable—
(1) ensure that the availability of Government information
and services has not been diminished for individuals who lack
access to the Internet; and
(2) pursue alternate modes of delivery that make Government

information and services more accessible to individuals
who do not own computers or lack access to the Internet.
(d) ACCESSIBILITY TO PEOPLE WITH DISABILITIES.—All actions
taken by Federal departments and agencies under this Act shall
be in compliance with section 508 of the Rehabilitation Act of
1973 (29 U.S.C. 794d).
(e) SPONSORED ACTIVITIES.—Agencies shall sponsor activities
that use information technology to engage the public in the development
and implementation of policies and programs.
44 USC 3501
note.

(f) CHIEF INFORMATION OFFICERS.—The Chief Information
Officer of each of the agencies designated under chapter 36 of
title 44, United States Code (as added by this Act) shall be responsible
for—
(1) participating in the functions of the Chief Information
Officers Council; and
(2) monitoring the implementation, within their respective
agencies, of information technology standards promulgated by
the Secretary of Commerce, including common standards for
interconnectivity and interoperability, categorization of Federal
Government electronic information, and computer system efficiency
and security.
(g) E-GOVERNMENT STATUS REPORT.—
(1) IN GENERAL.—Each agency shall compile and submit
to the Director an annual E-Government Status Report on—
(A) the status of the implementation by the agency

of electronic government initiatives;

(B) compliance by the agency with this Act; and

(C) how electronic Government initiatives of the agency improve performance in delivering programs to constituencies.

(2) SUBMISSION.—Each agency shall submit an annual report under this subsection—

(A) to the Director at such time and in such manner as the Director requires;

(B) consistent with related reporting requirements; and

(C) which addresses any section in this title relevant to that agency.

(h) USE OF TECHNOLOGY.—Nothing in this Act supersedes the responsibility of an agency to use or manage information technology to deliver Government information and services that fulfill the statutory mission and programs of the agency.

(i) NATIONAL SECURITY SYSTEMS.—

(1) INAPPLICABILITY.—Except as provided under paragraph (2), this title does not apply to national security systems as defined in section 11103 of title 40, United States Code.

(2) APPLICABILITY.—This section, section 203, and section 214 do apply to national security systems to the extent practicable and consistent with law.

SEC. 203. COMPATIBILITY OF EXECUTIVE AGENCY METHODS FOR USE AND ACCEPTANCE OF ELECTRONIC SIGNATURES.

(a) PURPOSE.—The purpose of this section is to achieve interoperable implementation of electronic signatures for appropriately secure electronic transactions with Government.

(b) ELECTRONIC SIGNATURES.—In order to fulfill the objectives of the Government Paperwork Elimination Act (Public Law 105–277; 112 Stat. 2681–749 through 2681–751), each Executive agency

(as defined under section 105 of title 5, United States Code) shall ensure that its methods for use and acceptance of electronic signatures are compatible with the relevant policies and procedures issued by the Director.

(c) AUTHORITY FOR ELECTRONIC SIGNATURES.—The Administrator of General Services shall support the Director by establishing a framework to allow efficient interoperability among Executive agencies when using electronic signatures, including processing of digital signatures.

44 USC 3501 note.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the General Services Administration, to ensure the development and operation of a Federal bridge certification authority for digital signature compatibility, and for other activities consistent with this section, $8,000,000 or such sums as are necessary in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

SEC. 204. FEDERAL INTERNET PORTAL.

(a) IN GENERAL.—

(1) PUBLIC ACCESS.—The Director shall work with the Administrator of the General Services Administration and other agencies to maintain and promote an integrated Internet-based system of providing the public with access to Government information and services.

(2) CRITERIA.—To the extent practicable, the integrated system shall be designed and operated according to the following

criteria:

(A) The provision of Internet-based Government information and services directed to key groups, including citizens, business, and other governments, and integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction.

(B) An ongoing effort to ensure that Internet-based Government services relevant to a given citizen activity are available from a single point.

(C) Access to Federal Government information and services consolidated, as appropriate, with Internet-based information and services provided by State, local, and tribal governments.

(D) Access to Federal Government information held by 1 or more agencies shall be made available in a manner that protects privacy, consistent with law.

(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the General Services Administration $15,000,000 for the maintenance, improvement, and promotion of the integrated Internet-based system for fiscal year 2003, and such sums as are necessary for fiscal years 2004 through 2007.

SEC. 205. FEDERAL COURTS.

(a) INDIVIDUAL COURT WEBSITES.—The Chief Justice of the United States, the chief judge of each circuit and district and of the Court of Federal Claims, and the chief bankruptcy judge of each district shall cause to be established and maintained, for the court of which the judge is chief justice or judge, a website that contains the following information or links to websites with the following information:

(1) Location and contact information for the courthouse,

including the telephone numbers and contact names for the clerk's office and justices' or judges' chambers.

(2) Local rules and standing or general orders of the court.

(3) Individual rules, if in existence, of each justice or judge in that court.

(4) Access to docket information for each case.

(5) Access to the substance of all written opinions issued by the court, regardless of whether such opinions are to be published in the official court reporter, in a text searchable format.

44 USC 3501 note.

44 USC 3501 note.

(6) Access to documents filed with the courthouse in electronic form, to the extent provided under subsection (c).

(7) Any other information (including forms in a format that can be downloaded) that the court determines useful to the public.

(b) MAINTENANCE OF DATA ONLINE.—

(1) UPDATE OF INFORMATION.—The information and rules on each website shall be updated regularly and kept reasonably current.

(2) CLOSED CASES.—Electronic files and docket information for cases closed for more than 1 year are not required to be made available online, except all written opinions with a date of issuance after the effective date of this section shall

remain available online.

(c) ELECTRONIC FILINGS.—

(1) IN GENERAL.—Except as provided under paragraph (2) or in the rules prescribed under paragraph (3), each court shall make any document that is filed electronically publicly available online. A court may convert any document that is filed in paper form to electronic form. To the extent such conversions are made, all such electronic versions of the document shall be made available online.

(2) EXCEPTIONS.—Documents that are filed that are not otherwise available to the public, such as documents filed under seal, shall not be made available online.

(3) PRIVACY AND SECURITY CONCERNS.—(A)(i) The Supreme Court shall prescribe rules, in accordance with sections 2072 and 2075 of title 28, United States Code, to protect privacy and security concerns relating to electronic filing of documents and the public availability under this subsection of documents filed electronically.

(ii) Such rules shall provide to the extent practicable for uniform treatment of privacy and security issues throughout the Federal courts.

(iii) Such rules shall take into consideration best practices in Federal and State courts to protect private information or otherwise maintain necessary information security.

(iv) To the extent that such rules provide for the redaction of certain categories of information in order to protect privacy and security concerns, such rules shall provide that a party that wishes to file an otherwise proper document containing such information may file an unredacted document under seal, which shall be retained by the court as part of the record,

and which, at the discretion of the court and subject to any applicable rules issued in accordance with chapter 131 of title 28, United States Code, shall be either in lieu of, or in addition, to, a redacted copy in the public file.

(B)(i) Subject to clause (ii), the Judicial Conference of the United States may issue interim rules, and interpretive statements relating to the application of such rules, which conform to the requirements of this paragraph and which shall cease to have effect upon the effective date of the rules required under subparagraph (A).

(ii) Pending issuance of the rules required under subparagraph (A), any rule or order of any court, or of the Judicial Conference, providing for the redaction of certain categories of information in order to protect privacy and security concerns

Regulations.

Public information.

arising from electronic filing shall comply with, and be construed in conformity with, subparagraph (A)(iv).

(C) Not later than 1 year after the rules prescribed under subparagraph (A) take effect, and every 2 years thereafter, the Judicial Conference shall submit to Congress a report on the adequacy of those rules to protect privacy and security.

(d) DOCKETS WITH LINKS TO DOCUMENTS.—The Judicial Conference of the United States shall explore the feasibility of technology to post online dockets with links allowing all filings, decisions, and rulings in each case to be obtained from the docket

sheet of that case.

(e) COST OF PROVIDING ELECTRONIC DOCKETING INFORMATION.—Section 303(a) of the Judiciary Appropriations Act, 1992 (28 U.S.C. 1913 note) is amended in the first sentence by striking ''shall hereafter'' and inserting ''may, only to the extent necessary,''.

(f) TIME REQUIREMENTS.—Not later than 2 years after the effective date of this title, the websites under subsection (a) shall be established, except that access to documents filed in electronic form shall be established not later than 4 years after that effective date.

(g) DEFERRAL.—

(1) IN GENERAL.—

(A) ELECTION.—

(i) NOTIFICATION.—The Chief Justice of the United States, a chief judge, or chief bankruptcy judge may submit a notification to the Administrative Office of the United States Courts to defer compliance with any requirement of this section with respect to the Supreme Court, a court of appeals, district, or the bankruptcy court of a district.

(ii) CONTENTS.—A notification submitted under this subparagraph shall state—

(I) the reasons for the deferral; and

(II) the online methods, if any, or any alternative methods, such court or district is using to provide greater public access to information.

(B) EXCEPTION.—To the extent that the Supreme Court, a court of appeals, district, or bankruptcy court of a district maintains a website under subsection (a), the Supreme Court or that court of appeals or district

shall comply with subsection (b)(1).

(2) REPORT.—Not later than 1 year after the effective date of this title, and every year thereafter, the Judicial Conference of the United States shall submit a report to the Committees on Governmental Affairs and the Judiciary of the Senate and the Committees on Government Reform and the Judiciary of the House of Representatives that—

(A) contains all notifications submitted to the Administrative Office of the United States Courts under this subsection; and

(B) summarizes and evaluates all notifications.

SEC. 206. REGULATORY AGENCIES.

(a) PURPOSES.—The purposes of this section are to—

(1) improve performance in the development and issuance of agency regulations by using information technology to increase access, accountability, and transparency; and

44 USC 3501 note.

Deadline.

Deadlines.

Deadlines.

Reports.

(2) enhance public participation in Government by electronic means, consistent with requirements under subchapter II of chapter 5 of title 5, United States Code, (commonly referred to as the ‘‘Administrative Procedures Act’’).

(b) INFORMATION PROVIDED BY AGENCIES ONLINE.—To the

extent practicable as determined by the agency in consultation with the Director, each agency (as defined under section 551 of title 5, United States Code) shall ensure that a publicly accessible Federal Government website includes all information about that agency required to be published in the Federal Register under paragraphs (1) and (2) of section 552(a) of title 5, United States Code.

(c) SUBMISSIONS BY ELECTRONIC MEANS.—To the extent practicable, agencies shall accept submissions under section 553(c) of title 5, United States Code, by electronic means.

(d) ELECTRONIC DOCKETING.—

(1) IN GENERAL.—To the extent practicable, as determined by the agency in consultation with the Director, agencies shall ensure that a publicly accessible Federal Government website contains electronic dockets for rulemakings under section 553 of title 5, United States Code.

(2) INFORMATION AVAILABLE.—Agency electronic dockets shall make publicly available online to the extent practicable, as determined by the agency in consultation with the Director—

(A) all submissions under section 553(c) of title 5, United States Code; and

(B) other materials that by agency rule or practice are included in the rulemaking docket under section 553(c) of title 5, United States Code, whether or not submitted electronically.

(e) TIME LIMITATION.—Agencies shall implement the requirements of this section consistent with a timetable established by the Director and reported to Congress in the first annual report under section 3606 of title 44 (as added by this Act).

SEC. 207. ACCESSIBILITY, USABILITY, AND PRESERVATION OF

GOVERNMENT INFORMATION.

(a) PURPOSE.—The purpose of this section is to improve the methods by which Government information, including information on the Internet, is organized, preserved, and made accessible to the public.

(b) DEFINITIONS.—In this section, the term—

(1) ''Committee'' means the Interagency Committee on Government Information established under subsection (c); and

(2) ''directory'' means a taxonomy of subjects linked to websites that—

(A) organizes Government information on the Internet according to subject matter; and

(B) may be created with the participation of human editors.

(c) INTERAGENCY COMMITTEE.—

(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this title, the Director shall establish the Interagency Committee on Government Information.

(2) MEMBERSHIP.—The Committee shall be chaired by the Director or the designee of the Director and—

(A) shall include representatives from—

Deadline.

44 USC 3501 note.

(i) the National Archives and Records Administration;

(ii) the offices of the Chief Information Officers from Federal agencies; and

(iii) other relevant officers from the executive
branch; and
(B) may include representatives from the Federal legislative
and judicial branches.
(3) FUNCTIONS.—The Committee shall—
(A) engage in public consultation to the maximum
extent feasible, including consultation with interested
communities such as public advocacy organizations;
(B) conduct studies and submit recommendations, as
provided under this section, to the Director and Congress;
and
(C) share effective practices for access to, dissemination
of, and retention of Federal information.
(4) TERMINATION.—The Committee may be terminated on
a date determined by the Director, except the Committee may
not terminate before the Committee submits all recommendations
required under this section.
(d) CATEGORIZING OF INFORMATION.—
(1) COMMITTEE FUNCTIONS.—Not later than 2 years after
the date of enactment of this Act, the Committee shall submit
recommendations to the Director on—
(A) the adoption of standards, which are open to the
maximum extent feasible, to enable the organization and
categorization of Government information—
(i) in a way that is searchable electronically,
including by searchable identifiers; and
(ii) in ways that are interoperable across agencies;
(B) the definition of categories of Government information
which should be classified under the standards; and
(C) determining priorities and developing schedules

for the initial implementation of the standards by agencies.

(2) FUNCTIONS OF THE DIRECTOR.—Not later than 1 year after the submission of recommendations under paragraph (1), the Director shall issue policies—

(A) requiring that agencies use standards, which are open to the maximum extent feasible, to enable the organization and categorization of Government information—

(i) in a way that is searchable electronically, including by searchable identifiers;

(ii) in ways that are interoperable across agencies; and

(iii) that are, as appropriate, consistent with the provisions under section 3602(f)(8) of title 44, United States Code;

(B) defining categories of Government information which shall be required to be classified under the standards; and

(C) determining priorities and developing schedules for the initial implementation of the standards by agencies.

(3) MODIFICATION OF POLICIES.—After the submission of agency reports under paragraph (4), the Director shall modify

Deadline.

Policies.

Deadline.

the policies, as needed, in consultation with the Committee and interested parties.

(4) AGENCY FUNCTIONS.—Each agency shall report annually to the Director, in the report established under section 202(g), on compliance of that agency with the policies issued under paragraph (2)(A).

(e) PUBLIC ACCESS TO ELECTRONIC INFORMATION.—

(1) COMMITTEE FUNCTIONS.—Not later than 2 years after the date of enactment of this Act, the Committee shall submit recommendations to the Director and the Archivist of the United States on—

(A) the adoption by agencies of policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records; and

(B) the imposition of timetables for the implementation of the policies and procedures by agencies.

(2) FUNCTIONS OF THE ARCHIVIST.—Not later than 1 year after the submission of recommendations by the Committee under paragraph (1), the Archivist of the United States shall issue policies—

(A) requiring the adoption by agencies of policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records; and

(B) imposing timetables for the implementation of the policies, procedures, and technologies by agencies.

(3) MODIFICATION OF POLICIES.—After the submission of agency reports under paragraph (4), the Archivist of the United States shall modify the policies, as needed, in consultation

with the Committee and interested parties.

(4) AGENCY FUNCTIONS.—Each agency shall report annually to the Director, in the report established under section 202(g), on compliance of that agency with the policies issued under paragraph (2)(A).

(f) AGENCY WEBSITES.—

(1) STANDARDS FOR AGENCY WEBSITES.—Not later than 2 years after the effective date of this title, the Director shall promulgate guidance for agency websites that includes—

(A) requirements that websites include direct links to—

(i) descriptions of the mission and statutory authority of the agency;

(ii) information made available to the public under subsections (a)(1) and (b) of section 552 of title 5, United States Code (commonly referred to as the ''Freedom of Information Act'');

(iii) information about the organizational structure of the agency; and

(iv) the strategic plan of the agency developed under section 306 of title 5, United States Code; and

(B) minimum agency goals to assist public users to navigate agency websites, including—

(i) speed of retrieval of search results;

(ii) the relevance of the results;

Deadline.

Guidelines.

Reports.

Deadline.

Policies.

Deadline.

Reports.

(iii) tools to aggregate and disaggregate data; and

(iv) security protocols to protect information.

(2) AGENCY REQUIREMENTS.—(A) Not later than 2 years after the date of enactment of this Act, each agency shall—

(i) consult with the Committee and solicit public comment;

(ii) establish a process for determining which Government information the agency intends to make available and accessible to the public on the Internet and by other means;

(iii) develop priorities and schedules for making Government information available and accessible;

(iv) make such final determinations, priorities, and schedules available for public comment;

(v) post such final determinations, priorities, and schedules on the Internet; and

(vi) submit such final determinations, priorities, and schedules to the Director, in the report established under section 202(g).

(B) Each agency shall update determinations, priorities, and schedules of the agency, as needed, after consulting with the Committee and soliciting public comment, if appropriate.

(3) PUBLIC DOMAIN DIRECTORY OF PUBLIC FEDERAL GOVERNMENT WEBSITES.—

(A) ESTABLISHMENT.—Not later than 2 years after the effective date of this title, the Director and each agency

shall—
(i) develop and establish a public domain directory
of public Federal Government websites; and
(ii) post the directory on the Internet with a link
to the integrated Internet-based system established
under section 204.
(B) DEVELOPMENT.—With the assistance of each
agency, the Director shall—
(i) direct the development of the directory through
a collaborative effort, including input from—
(I) agency librarians;
(II) information technology managers;
(III) program managers;
(IV) records managers;
(V) Federal depository librarians; and
(VI) other interested parties; and
(ii) develop a public domain taxonomy of subjects
used to review and categorize public Federal Government
websites.
(C) UPDATE.—With the assistance of each agency, the
Administrator of the Office of Electronic Government
shall—
(i) update the directory as necessary, but not less
than every 6 months; and
(ii) solicit interested persons for improvements to
the directory.
(g) ACCESS TO FEDERALLY FUNDED RESEARCH AND DEVELOPMENT.—
(1) DEVELOPMENT AND MAINTENANCE OF GOVERNMENTWIDE
REPOSITORY AND WEBSITE.—
Deadline.

Deadline.

Deadline.

(A) REPOSITORY AND WEBSITE.—The Director of the Office of Management and Budget (or the Director's delegate), in consultation with the Director of the Office of Science and Technology Policy and other relevant agencies, shall ensure the development and maintenance of—

(i) a repository that fully integrates, to the maximum extent feasible, information about research and development funded by the Federal Government, and the repository shall—

(I) include information about research and development funded by the Federal Government, consistent with any relevant protections for the information under section 552 of title 5, United States Code, and performed by—

(aa) institutions not a part of the Federal Government, including State, local, and foreign governments; industrial firms; educational institutions; not-for-profit organizations; federally funded research and development centers; and private individuals; and

(bb) entities of the Federal Government, including research and development laboratories, centers, and offices; and

(II) integrate information about each separate research and development task or award,

including—
(aa) the dates upon which the task or
award is expected to start and end;
(bb) a brief summary describing the objective
and the scientific and technical focus of
the task or award;
(cc) the entity or institution performing
the task or award and its contact information;
(dd) the total amount of Federal funds
expected to be provided to the task or award
over its lifetime and the amount of funds
expected to be provided in each fiscal year
in which the work of the task or award is
ongoing;
(ee) any restrictions attached to the task
or award that would prevent the sharing with
the general public of any or all of the information
required by this subsection, and the reasons
for such restrictions; and
(ff) such other information as may be
determined to be appropriate; and
(ii) 1 or more websites upon which all or part
of the repository of Federal research and development
shall be made available to and searchable by Federal
agencies and non-Federal entities, including the general
public, to facilitate—
(I) the coordination of Federal research and
development activities;
(II) collaboration among those conducting Federal
research and development;

Public
information.

(III) the transfer of technology among Federal agencies and between Federal agencies and non-Federal entities; and

(IV) access by policymakers and the public to information concerning Federal research and development activities.

(B) OVERSIGHT.—The Director of the Office of Management and Budget shall issue any guidance determined necessary to ensure that agencies provide all information requested under this subsection.

(2) AGENCY FUNCTIONS.—Any agency that funds Federal research and development under this subsection shall provide the information required to populate the repository in the manner prescribed by the Director of the Office of Management and Budget.

(3) COMMITTEE FUNCTIONS.—Not later than 18 months after the date of enactment of this Act, working with the Director of the Office of Science and Technology Policy, and after consultation with interested parties, the Committee shall submit recommendations to the Director on—

(A) policies to improve agency reporting of information for the repository established under this subsection; and

(B) policies to improve dissemination of the results of research performed by Federal agencies and federally funded research and development centers.

(4) FUNCTIONS OF THE DIRECTOR.—After submission of recommendations by the Committee under paragraph (3), the Director shall report on the recommendations of the Committee and Director to Congress, in the E-Government report under section 3606 of title 44 (as added by this Act).

(5) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the development, maintenance, and operation of the Governmentwide repository and website under this subsection—

(A) $2,000,000 in each of the fiscal years 2003 through 2005; and

(B) such sums as are necessary in each of the fiscal years 2006 and 2007.

SEC. 208. PRIVACY PROVISIONS.

(a) PURPOSE.—The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

(b) PRIVACY IMPACT ASSESSMENTS.—

(1) RESPONSIBILITIES OF AGENCIES.—

(A) IN GENERAL.—An agency shall take actions described under subparagraph (B) before—

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

(ii) initiating a new collection of information that—

(I) will be collected, maintained, or disseminated using information technology; and

(II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have

been posed to, or identical reporting requirements

44 USC 3501 note.

Reports.

Deadline.

Guidelines.

imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

(B) AGENCY ACTIVITIES.—To the extent required under subparagraph (A), each agency shall—

(i) conduct a privacy impact assessment;

(ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and

(iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

(C) SENSITIVE INFORMATION.—Subparagraph (B)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

(D) COPY TO DIRECTOR.—Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

(2) CONTENTS OF A PRIVACY IMPACT ASSESSMENT.—

(A) IN GENERAL.—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

(B) GUIDANCE.—The guidance shall—

(i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and

(ii) require that a privacy impact assessment address—

(I) what information is to be collected;

(II) why the information is being collected;

(III) the intended use of the agency of the information;

(IV) with whom the information will be shared;

(V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(VI) how the information will be secured; and

(VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the ‘‘Privacy Act’’).

(3) RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—

(A) develop policies and guidelines for agencies on the conduct of privacy impact assessments;

(B) oversee the implementation of the privacy impact

assessment process throughout the Government; and

(C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

(c) PRIVACY PROTECTIONS ON AGENCY WEBSITES.—

Guidelines.

Public information.

Federal Register, publication.

(1) PRIVACY POLICIES ON WEBSITES.—

(A) GUIDELINES FOR NOTICES.—The Director shall develop guidance for privacy notices on agency websites used by the public.

(B) CONTENTS.—The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—

(i) what information is to be collected;

(ii) why the information is being collected;

(iii) the intended use of the agency of the information;

(iv) with whom the information will be shared;

(v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(vi) how the information will be secured; and

(vii) the rights of the individual under section 552a

of title 5, United States Code (commonly referred to as the ‘‘Privacy Act’’), and other laws relevant to the protection of the privacy of an individual.

(2) PRIVACY POLICIES IN MACHINE-READABLE FORMATS.—The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

(d) DEFINITION.—In this section, the term ‘‘identifiable form’’ means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

SEC. 209. FEDERAL INFORMATION TECHNOLOGY WORKFORCE DEVELOPMENT.

(a) PURPOSE.—The purpose of this section is to improve the skills of the Federal workforce in using information technology to deliver Government information and services.

(b) WORKFORCE DEVELOPMENT.—

(1) IN GENERAL.—In consultation with the Director of the Office of Management and Budget, the Chief Information Officers Council, and the Administrator of General Services, the Director of the Office of Personnel Management shall—

(A) analyze, on an ongoing basis, the personnel needs of the Federal Government related to information technology and information resource management;

(B) identify where current information technology and information resource management training do not satisfy the personnel needs described in subparagraph (A);

(C) oversee the development of curricula, training methods, and training priorities that correspond to the projected personnel needs of the Federal Government related to information technology and information resource

management; and

(D) assess the training of Federal employees in information technology disciplines in order to ensure that the information resource management needs of the Federal Government are addressed.

(2) INFORMATION TECHNOLOGY TRAINING PROGRAMS.—The head of each Executive agency, after consultation with the Director of the Office of Personnel Management, the Chief

44 USC 3501 note.

Guidelines.

Information Officers Council, and the Administrator of General Services, shall establish and operate information technology training programs consistent with the requirements of this subsection. Such programs shall—

(A) have curricula covering a broad range of information technology disciplines corresponding to the specific information technology and information resource management needs of the agency involved;

(B) be developed and applied according to rigorous standards; and

(C) be designed to maximize efficiency, through the use of self-paced courses, online courses, on-the-job training, and the use of remote instructors, wherever such features can be applied without reducing the effectiveness of the training or negatively impacting academic standards.

(3) GOVERNMENTWIDE POLICIES AND EVALUATION.—The

Director of the Office of Personnel Management, in coordination with the Director of the Office of Management and Budget, shall issue policies to promote the development of performance standards for training and uniform implementation of this subsection by Executive agencies, with due regard for differences in program requirements among agencies that may be appropriate and warranted in view of the agency mission. The Director of the Office of Personnel Management shall evaluate the implementation of the provisions of this subsection by Executive agencies.

(4) CHIEF INFORMATION OFFICER AUTHORITIES AND RESPONSIBILITIES.—Subject to the authority, direction, and control of the head of an Executive agency, the chief information officer of such agency shall carry out all powers, functions, and duties of the head of the agency with respect to implementation of this subsection. The chief information officer shall ensure that the policies of the agency head established in accordance with this subsection are implemented throughout the agency.

(5) INFORMATION TECHNOLOGY TRAINING REPORTING.—The Director of the Office of Management and Budget shall ensure that the heads of Executive agencies collect and maintain standardized information on the information technology and information resources management workforce related to the implementation of this subsection.

(6) AUTHORITY TO DETAIL EMPLOYEES TO NON-FEDERAL EMPLOYERS.—In carrying out the preceding provisions of this subsection, the Director of the Office of Personnel Management may provide for a program under which a Federal employee may be detailed to a non-Federal employer. The Director of the Office of Personnel Management shall prescribe regulations

for such program, including the conditions for service and duties as the Director considers necessary.

(7) COORDINATION PROVISION.—An assignment described in section 3703 of title 5, United States Code, may not be made unless a program under paragraph (6) is established, and the assignment is made in accordance with the requirements of such program.

(8) EMPLOYEE PARTICIPATION.—Subject to information resource management needs and the limitations imposed by resource needs in other occupational areas, and consistent with their overall workforce development strategies, agencies shall

Regulations.

Records.

encourage employees to participate in occupational information technology training.

(9) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Office of Personnel Management for the implementation of this subsection, $15,000,000 in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

(10) EXECUTIVE AGENCY DEFINED.—For purposes of this subsection, the term ''Executive agency'' has the meaning given the term ''agency'' under section 3701 of title 5, United States Code (as added by subsection (c)).

(c) INFORMATION TECHNOLOGY EXCHANGE PROGRAM.—

(1) IN GENERAL.—Subpart B of part III of title 5, United States Code, is amended by adding at the end the following:

‘‘CHAPTER 37—INFORMATION TECHNOLOGY EXCHANGE PROGRAM

‘‘Sec.

‘‘3701. Definitions.

‘‘3702. General provisions.

‘‘3703. Assignment of employees to private sector organizations.

‘‘3704. Assignment of employees from private sector organizations.

‘‘3705. Application to Office of the Chief Technology Officer of the District of Columbia.

‘‘3706. Reporting requirement.

‘‘3707. Regulations.

‘‘§ 3701. Definitions

‘‘For purposes of this chapter—

‘‘(1) the term ‘agency’ means an Executive agency, but does not include the General Accounting Office; and

‘‘(2) the term ‘detail’ means—

‘‘(A) the assignment or loan of an employee of an agency to a private sector organization without a change of position from the agency that employs the individual, or

‘‘(B) the assignment or loan of an employee of a private sector organization to an agency without a change of position from the private sector organization that employs the individual,

whichever is appropriate in the context in which such term is used.

‘‘§ 3702. General provisions

‘‘(a) ASSIGNMENT AUTHORITY.—On request from or with the agreement of a private sector organization, and with the consent of the employee concerned, the head of an agency may arrange for the assignment of an employee of the agency to a private

sector organization or an employee of a private sector organization
to the agency. An eligible employee is an individual who—
‘‘(1) works in the field of information technology management;
‘‘(2) is considered an exceptional performer by the individual’s
current employer; and
‘‘(3) is expected to assume increased information technology
management responsibilities in the future.
An employee of an agency shall be eligible to participate in this
program only if the employee is employed at the GS–11 level
Eligibility.

or above (or equivalent) and is serving under a career or careerconditional
appointment or an appointment of equivalent tenure
in the excepted service, and applicable requirements of section
209(b) of the E-Government Act of 2002 are met with respect
to the proposed assignment of such employee.
‘‘(b) AGREEMENTS.—Each agency that exercises its authority
under this chapter shall provide for a written agreement between
the agency and the employee concerned regarding the terms and
conditions of the employee’s assignment. In the case of an employee
of the agency, the agreement shall—
‘‘(1) require the employee to serve in the civil service,
upon completion of the assignment, for a period equal to the
length of the assignment; and
‘‘(2) provide that, in the event the employee fails to carry
out the agreement (except for good and sufficient reason, as
determined by the head of the agency from which assigned)
the employee shall be liable to the United States for payment

of all expenses of the assignment.
An amount under paragraph (2) shall be treated as a debt due the United States.
‘‘(c) TERMINATION.—Assignments may be terminated by the agency or private sector organization concerned for any reason at any time.
‘‘(d) DURATION.—Assignments under this chapter shall be for a period of between 3 months and 1 year, and may be extended in 3-month increments for a total of not more than 1 additional year, except that no assignment under this chapter may commence after the end of the 5-year period beginning on the date of the enactment of this chapter.
‘‘(e) ASSISTANCE.—The Chief Information Officers Council, by agreement with the Office of Personnel Management, may assist in the administration of this chapter, including by maintaining lists of potential candidates for assignment under this chapter, establishing mentoring relationships for the benefit of individuals who are given assignments under this chapter, and publicizing the program.
‘‘(f) CONSIDERATIONS.—In exercising any authority under this chapter, an agency shall take into consideration—
‘‘(1) the need to ensure that small business concerns are appropriately represented with respect to the assignments described in sections 3703 and 3704, respectively; and
‘‘(2) how assignments described in section 3703 might best be used to help meet the needs of the agency for the training of employees in information technology management.
‘‘§ 3703. Assignment of employees to private sector organizations
‘‘(a) IN GENERAL.—An employee of an agency assigned to a private sector organization under this chapter is deemed, during

the period of the assignment, to be on detail to a regular work assignment in his agency.

''(b) COORDINATION WITH CHAPTER 81.—Notwithstanding any other provision of law, an employee of an agency assigned to a private sector organization under this chapter is entitled to retain coverage, rights, and benefits under subchapter I of chapter 81, and employment during the assignment is deemed employment by the United States, except that, if the employee or the employee's

dependents receive from the private sector organization any payment under an insurance policy for which the premium is wholly paid by the private sector organization, or other benefit of any kind on account of the same injury or death, then, the amount of such payment or benefit shall be credited against any compensation otherwise payable under subchapter I of chapter 81.

''(c) REIMBURSEMENTS.—The assignment of an employee to a private sector organization under this chapter may be made with or without reimbursement by the private sector organization for the travel and transportation expenses to or from the place of assignment, subject to the same terms and conditions as apply with respect to an employee of a Federal agency or a State or local government under section 3375, and for the pay, or a part thereof, of the employee during assignment. Any reimbursements shall be credited to the appropriation of the agency used for paying the travel and transportation expenses or pay.

''(d) TORT LIABILITY; SUPERVISION.—The Federal Tort Claims Act and any other Federal tort liability statute apply to an employee of an agency assigned to a private sector organization under this

chapter. The supervision of the duties of an employee of an agency so assigned to a private sector organization may be governed by an agreement between the agency and the organization.

''(e) SMALL BUSINESS CONCERNS.—

''(1) IN GENERAL.—The head of each agency shall take such actions as may be necessary to ensure that, of the assignments made under this chapter from such agency to private sector organizations in each year, at least 20 percent are to small business concerns.

''(2) DEFINITIONS.—For purposes of this subsection—

''(A) the term 'small business concern' means a business concern that satisfies the definitions and standards specified by the Administrator of the Small Business Administration under section 3(a)(2) of the Small Business Act (as from time to time amended by the Administrator);

''(B) the term 'year' refers to the 12-month period beginning on the date of the enactment of this chapter, and each succeeding 12-month period in which any assignments under this chapter may be made; and

''(C) the assignments 'made' in a year are those commencing in such year.

''(3) REPORTING REQUIREMENT.—An agency which fails to comply with paragraph (1) in a year shall, within 90 days after the end of such year, submit a report to the Committees on Government Reform and Small Business of the House of Representatives and the Committees on Governmental Affairs and Small Business of the Senate. The report shall include—

''(A) the total number of assignments made under this chapter from such agency to private sector organizations in the year;

‘‘(B) of that total number, the number (and percentage) made to small business concerns; and

‘‘(C) the reasons for the agency’s noncompliance with paragraph (1).

‘‘(4) EXCLUSION.—This subsection shall not apply to an agency in any year in which it makes fewer than 5 assignments under this chapter to private sector organizations.

Deadline.

116 STAT. 2928 PUBLIC LAW 107–347—DEC. 17 2002

‘‘§ 3704. Assignment of employees from private sector organizations

‘‘(a) IN GENERAL.—An employee of a private sector organization assigned to an agency under this chapter is deemed, during the period of the assignment, to be on detail to such agency.

‘‘(b) TERMS AND CONDITIONS.—An employee of a private sector organization assigned to an agency under this chapter—

‘‘(1) may continue to receive pay and benefits from the private sector organization from which he is assigned;

‘‘(2) is deemed, notwithstanding subsection (a), to be an employee of the agency for the purposes of—

‘‘(A) chapter 73;

‘‘(B) sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18;

‘‘(C) sections 1343, 1344, and 1349(b) of title 31;

‘‘(D) the Federal Tort Claims Act and any other Federal tort liability statute;

‘‘(E) the Ethics in Government Act of 1978;

‘‘(F) section 1043 of the Internal Revenue Code of 1986;

and
‘‘(G) section 27 of the Office of Federal Procurement
Policy Act;
‘‘(3) may not have access to any trade secrets or to any
other nonpublic information which is of commercial value to
the private sector organization from which he is assigned; and
‘‘(4) is subject to such regulations as the President may
prescribe.
The supervision of an employee of a private sector organization
assigned to an agency under this chapter may be governed by
agreement between the agency and the private sector organization
concerned. Such an assignment may be made with or without
reimbursement by the agency for the pay, or a part thereof, of
the employee during the period of assignment, or for any contribution
of the private sector organization to employee benefit systems.
‘‘(c) COORDINATION WITH CHAPTER 81.—An employee of a private
sector organization assigned to an agency under this chapter
who suffers disability or dies as a result of personal injury sustained
while performing duties during the assignment shall be treated,
for the purpose of subchapter I of chapter 81, as an employee
as defined by section 8101 who had sustained the injury in the
performance of duty, except that, if the employee or the employee’s
dependents receive from the private sector organization any payment
under an insurance policy for which the premium is wholly
paid by the private sector organization, or other benefit of any
kind on account of the same injury or death, then, the amount
of such payment or benefit shall be credited against any compensation
otherwise payable under subchapter I of chapter 81.
‘‘(d) PROHIBITION AGAINST CHARGING CERTAIN COSTS TO THE
FEDERAL GOVERNMENT.—A private sector organization may not

charge the Federal Government, as direct or indirect costs under a Federal contract, the costs of pay or benefits paid by the organization to an employee assigned to an agency under this chapter for the period of the assignment.

''§ 3705. Application to Office of the Chief Technology Officer of the District of Columbia

''(a) IN GENERAL.—The Chief Technology Officer of the District of Columbia may arrange for the assignment of an employee of the Office of the Chief Technology Officer to a private sector organization, or an employee of a private sector organization to such Office, in the same manner as the head of an agency under this chapter.

''(b) TERMS AND CONDITIONS.—An assignment made pursuant to subsection (a) shall be subject to the same terms and conditions as an assignment made by the head of an agency under this chapter, except that in applying such terms and conditions to an assignment made pursuant to subsection (a), any reference in this chapter to a provision of law or regulation of the United States shall be deemed to be a reference to the applicable provision of law or regulation of the District of Columbia, including the applicable provisions of the District of Columbia Government Comprehensive Merit Personnel Act of 1978 (sec. 1–601.01 et seq., D.C. Official Code) and section 601 of the District of Columbia Campaign Finance Reform and Conflict of Interest Act (sec. 1–1106.01, D.C. Official Code).

''(c) DEFINITION.—For purposes of this section, the term 'Office of the Chief Technology Officer' means the office established in

the executive branch of the government of the District of Columbia under the Office of the Chief Technology Officer Establishment Act of 1998 (sec. 1–1401 et seq., D.C. Official Code).

‘‘§ 3706. Reporting requirement

‘‘(a) IN GENERAL.—The Office of Personnel Management shall, not later than April 30 and October 31 of each year, prepare and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a semiannual report summarizing the operation of this chapter during the immediately preceding 6-month period ending on March 31 and September 30, respectively.

‘‘(b) CONTENT.—Each report shall include, with respect to the 6-month period to which such report relates—

‘‘(1) the total number of individuals assigned to, and the total number of individuals assigned from, each agency during such period;

‘‘(2) a brief description of each assignment included under paragraph (1), including—

‘‘(A) the name of the assigned individual, as well as the private sector organization and the agency (including the specific bureau or other agency component) to or from which such individual was assigned;

‘‘(B) the respective positions to and from which the individual was assigned, including the duties and responsibilities and the pay grade or level associated with each; and

‘‘(C) the duration and objectives of the individual’s assignment; and

‘‘(3) such other information as the Office considers appropriate.

‘‘(c) PUBLICATION.—A copy of each report submitted under subsection

(a)—

‘‘(1) shall be published in the Federal Register; and Federal Register, publication.

Deadline.

‘‘(2) shall be made publicly available on the Internet.

‘‘(d) AGENCY COOPERATION.—On request of the Office, agencies shall furnish such information and reports as the Office may require in order to carry out this section.

‘‘§ 3707. Regulations

‘‘The Director of the Office of Personnel Management shall prescribe regulations for the administration of this chapter.’’.

(2) REPORT.—Not later than 4 years after the date of the enactment of this Act, the General Accounting Office shall prepare and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a report on the operation of chapter 37 of title 5, United States Code (as added by this subsection). Such report shall include—

(A) an evaluation of the effectiveness of the program established by such chapter; and

(B) a recommendation as to whether such program should be continued (with or without modification) or allowed to lapse.

(3) CLERICAL AMENDMENT.—The analysis for part III of title 5, United States Code, is amended by inserting after the item relating to chapter 35 the following:

‘‘37. Information Technology Exchange Program ..... 3701’’.

(d) ETHICS PROVISIONS.—

(1) ONE-YEAR RESTRICTION ON CERTAIN COMMUNICATIONS.—Section 207(c)(2)(A) of title 18, United States Code, is amended—

(A) by striking ‘‘or’’ at the end of clause (iii);

(B) by striking the period at the end of clause (iv) and inserting ‘‘; or’’; and

(C) by adding at the end the following:

‘‘(v) assigned from a private sector organization to an agency under chapter 37 of title 5.’’.

(2) DISCLOSURE OF CONFIDENTIAL INFORMATION.—Section 1905 of title 18, United States Code, is amended by inserting ‘‘or being an employee of a private sector organization who is or was assigned to an agency under chapter 37 of title 5,’’ after ‘‘(15 U.S.C. 1311–1314),’’.

(3) CONTRACT ADVICE.—Section 207 of title 18, United States Code, is amended by adding at the end the following:

‘‘(l) CONTRACT ADVICE BY FORMER DETAILS.—Whoever, being an employee of a private sector organization assigned to an agency under chapter 37 of title 5, within one year after the end of that assignment, knowingly represents or aids, counsels, or assists in representing any other person (except the United States) in connection with any contract with that agency shall be punished as provided in section 216 of this title.’’.

(4) RESTRICTION ON DISCLOSURE OF PROCUREMENT INFORMATION.—Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. 423) is amended in subsection (a)(1) by adding at the end the following new sentence: ‘‘In the case of an employee of a private sector organization assigned to an agency under chapter 37 of title 5, United States Code, in addition

to the restriction in the preceding sentence, such employee shall not, other than as provided by law, knowingly disclose contractor bid or proposal information or source selection information during the three-year period after the end of the assignment of such employee.''.

Deadline.

Public information.

(e) REPORT ON EXISTING EXCHANGE PROGRAMS.—

(1) EXCHANGE PROGRAM DEFINED.—For purposes of this subsection, the term ''exchange program'' means an executive exchange program, the program under subchapter VI of chapter 33 of title 5, United States Code, and any other program which allows for—

(A) the assignment of employees of the Federal Government to non-Federal employers;

(B) the assignment of employees of non-Federal employers to the Federal Government; or

(C) both.

(2) REPORTING REQUIREMENT.—Not later than 1 year after the date of the enactment of this Act, the Office of Personnel Management shall prepare and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a report identifying all existing exchange programs.

(3) SPECIFIC INFORMATION.—The report shall, for each such program, include—

(A) a brief description of the program, including its size, eligibility requirements, and terms or conditions for participation;
(B) specific citation to the law or other authority under which the program is established;
(C) the names of persons to contact for more information, and how they may be reached; and
(D) any other information which the Office considers appropriate.
(f) REPORT ON THE ESTABLISHMENT OF A GOVERNMENTWIDE INFORMATION TECHNOLOGY TRAINING PROGRAM.—
(1) IN GENERAL.—Not later January 1, 2003, the Office of Personnel Management, in consultation with the Chief Information Officers Council and the Administrator of General Services, shall review and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a written report on the following:
(A) The adequacy of any existing information technology training programs available to Federal employees on a Governmentwide basis.
(B)(i) If one or more such programs already exist, recommendations as to how they might be improved.
(ii) If no such program yet exists, recommendations as to how such a program might be designed and established.
(C) With respect to any recommendations under subparagraph (B), how the program under chapter 37 of title 5, United States Code, might be used to help carry them out.
(2) COST ESTIMATE.—The report shall, for any recommended

program (or improvements) under paragraph (1)(B), include the estimated costs associated with the implementation and operation of such program as so established (or estimated difference in costs of any such program as so improved).

(g) TECHNICAL AND CONFORMING AMENDMENTS.—

Deadline.

Deadline.

(1) AMENDMENTS TO TITLE 5, UNITED STATES CODE.—Title 5, United States Code, is amended—

(A) in section 3111, by adding at the end the following:

‘‘(d) Notwithstanding section 1342 of title 31, the head of an agency may accept voluntary service for the United States under chapter 37 of this title and regulations of the Office of Personnel Management.’’;

(B) in section 4108, by striking subsection (d); and

(C) in section 7353(b), by adding at the end the following:

‘‘(4) Nothing in this section precludes an employee of a private sector organization, while assigned to an agency under chapter 37, from continuing to receive pay and benefits from such organization in accordance with such chapter.’’.

(2) AMENDMENT TO TITLE 18, UNITED STATES CODE.—Section 209 of title 18, United States Code, is amended by adding at the end the following:

‘‘(g)(1) This section does not prohibit an employee of a private sector organization, while assigned to an agency under chapter 37 of title 5, from continuing to receive pay and benefits from such organization in accordance with such chapter.

‘‘(2) For purposes of this subsection, the term ‘agency’ means an agency (as defined by section 3701 of title 5) and the Office of the Chief Technology Officer of the District of Columbia.’’.

(3) OTHER AMENDMENTS.—Section 125(c)(1) of Public Law 100–238 (5 U.S.C. 8432 note) is amended—

(A) in subparagraph (B), by striking ‘‘or’’ at the end;

(B) in subparagraph (C), by striking ‘‘and’’ at the end and inserting ‘‘or’’; and

(C) by adding at the end the following:

‘‘(D) an individual assigned from a Federal agency to a private sector organization under chapter 37 of title 5, United States Code; and’’.

SEC. 210. SHARE-IN-SAVINGS INITIATIVES.

(a) DEFENSE CONTRACTS.—(1) Chapter 137 of title 10, United States Code, is amended by adding at the end the following new section:

‘‘§ 2332. Share-in-savings contracts

‘‘(a) AUTHORITY TO ENTER INTO SHARE-IN-SAVINGS CONTRACTS.—(1) The head of an agency may enter into a share-insavings contract for information technology (as defined in section 11101(6) of title 40) in which the Government awards a contract to improve mission-related or administrative processes or to accelerate the achievement of its mission and share with the contractor in savings achieved through contract performance.

‘‘(2)(A) Except as provided in subparagraph (B), a share-insavings contract shall be awarded for a period of not more than five years.

‘‘(B) A share-in-savings contract may be awarded for a period greater than five years, but not more than 10 years, if the head of the agency determines in writing prior to award of the contract

that—

‘‘(i) the level of risk to be assumed and the investment to be undertaken by the contractor is likely to inhibit the government from obtaining the needed information technology

44 USC 3501 note.

competitively at a fair and reasonable price if the contract is limited in duration to a period of five years or less; and

‘‘(ii) usage of the information technology to be acquired is likely to continue for a period of time sufficient to generate reasonable benefit for the government.

‘‘(3) Contracts awarded pursuant to the authority of this section shall, to the maximum extent practicable, be performance-based contracts that identify objective outcomes and contain performance standards that will be used to measure achievement and milestones that must be met before payment is made.

‘‘(4) Contracts awarded pursuant to the authority of this section shall include a provision containing a quantifiable baseline that is to be the basis upon which a savings share ratio is established that governs the amount of payment a contractor is to receive under the contract. Before commencement of performance of such a contract, the senior procurement executive of the agency shall determine in writing that the terms of the provision are quantifiable and will likely yield value to the Government.

‘‘(5)(A) The head of the agency may retain savings realized through the use of a share-in-savings contract under this section that are in excess of the total amount of savings paid to the

contractor under the contract, but may not retain any portion of such savings that is attributable to a decrease in the number of civilian employees of the Federal Government performing the function. Except as provided in subparagraph (B), savings shall be credited to the appropriation or fund against which charges were made to carry out the contract and shall be used for information technology.

‘‘(B) Amounts retained by the agency under this subsection shall—

‘‘(i) without further appropriation, remain available until expended; and

‘‘(ii) be applied first to fund any contingent liabilities associated with share-in-savings procurements that are not fully funded.

‘‘(b) CANCELLATION AND TERMINATION.—(1) If funds are not made available for the continuation of a share-in-savings contract entered into under this section in a subsequent fiscal year, the contract shall be canceled or terminated. The costs of cancellation or termination may be paid out of—

‘‘(A) appropriations available for the performance of the contract;

‘‘(B) appropriations available for acquisition of the information technology procured under the contract, and not otherwise obligated; or

‘‘(C) funds subsequently appropriated for payments of costs of cancellation or termination, subject to the limitations in paragraph (3).

‘‘(2) The amount payable in the event of cancellation or termination of a share-in-savings contract shall be negotiated with the contractor at the time the contract is entered into.

‘‘(3)(A) Subject to subparagraph (B), the head of an agency may enter into share-in-savings contracts under this section in any given fiscal year even if funds are not made specifically available for the full costs of cancellation or termination of the contract if funds are available and sufficient to make payments with respect to the first fiscal year of the contract and the following conditions

are met regarding the funding of cancellation and termination liability:

‘‘(i) The amount of unfunded contingent liability for the contract does not exceed the lesser of—

‘‘(I) 25 percent of the estimated costs of a cancellation or termination; or

‘‘(II) $5,000,000.

‘‘(ii) Unfunded contingent liability in excess of $1,000,000 has been approved by the Director of the Office of Management and Budget or the Director’s designee.

‘‘(B) The aggregate number of share-in-savings contracts that may be entered into under subparagraph (A) by all agencies to which this chapter applies in a fiscal year may not exceed 5 in each of fiscal years 2003, 2004, and 2005.

‘‘(c) DEFINITIONS.—In this section:

‘‘(1) The term ‘contractor’ means a private entity that enters into a contract with an agency.

‘‘(2) The term ‘savings’ means—

‘‘(A) monetary savings to an agency; or

‘‘(B) savings in time or other benefits realized by the agency, including enhanced revenues (other than enhanced

revenues from the collection of fees, taxes, debts, claims, or other amounts owed the Federal Government).

''(3) The term 'share-in-savings contract' means a contract under which—

''(A) a contractor provides solutions for—

''(i) improving the agency's mission-related or administrative processes; or

''(ii) accelerating the achievement of agency missions; and

''(B) the head of the agency pays the contractor an amount equal to a portion of the savings derived by the agency from—

''(i) any improvements in mission-related or administrative processes that result from implementation of the solution; or

''(ii) acceleration of achievement of agency missions.

''(d) TERMINATION.—No share-in-savings contracts may be entered into under this section after September 30, 2005.''.

(2) The table of sections at the beginning of such chapter is amended by adding at the end of the following new item:

''2332. Share-in-savings contracts.''.

(b) OTHER CONTRACTS.—Title III of the Federal Property and Administrative Services Act of 1949 is amended by adding at the end the following:

''SEC. 317. SHARE-IN-SAVINGS CONTRACTS.

''(a) AUTHORITY TO ENTER INTO SHARE-IN-SAVINGS CONTRACTS.—(1) The head of an executive agency may enter into a share-in-savings contract for information technology (as defined in section 11101(6) of title 40, United States Code) in which the Government awards a contract to improve mission-related or

administrative processes or to accelerate the achievement of its mission and share with the contractor in savings achieved through contract performance.

41 USC 266a.

''(2)(A) Except as provided in subparagraph (B), a share-insavings contract shall be awarded for a period of not more than five years.

''(B) A share-in-savings contract may be awarded for a period greater than five years, but not more than 10 years, if the head of the agency determines in writing prior to award of the contract that—

''(i) the level of risk to be assumed and the investment to be undertaken by the contractor is likely to inhibit the government from obtaining the needed information technology competitively at a fair and reasonable price if the contract is limited in duration to a period of five years or less; and

''(ii) usage of the information technology to be acquired is likely to continue for a period of time sufficient to generate reasonable benefit for the government.

''(3) Contracts awarded pursuant to the authority of this section shall, to the maximum extent practicable, be performance-based contracts that identify objective outcomes and contain performance standards that will be used to measure achievement and milestones that must be met before payment is made.

''(4) Contracts awarded pursuant to the authority of this section shall include a provision containing a quantifiable baseline that is to be the basis upon which a savings share ratio is established

that governs the amount of payment a contractor is to receive under the contract. Before commencement of performance of such a contract, the senior procurement executive of the agency shall determine in writing that the terms of the provision are quantifiable and will likely yield value to the Government.

''(5)(A) The head of the agency may retain savings realized through the use of a share-in-savings contract under this section that are in excess of the total amount of savings paid to the contractor under the contract, but may not retain any portion of such savings that is attributable to a decrease in the number of civilian employees of the Federal Government performing the function. Except as provided in subparagraph (B), savings shall be credited to the appropriation or fund against which charges were made to carry out the contract and shall be used for information technology.

''(B) Amounts retained by the agency under this subsection shall—

''(i) without further appropriation, remain available until expended; and

''(ii) be applied first to fund any contingent liabilities associated with share-in-savings procurements that are not fully funded.

''(b) CANCELLATION AND TERMINATION.—(1) If funds are not made available for the continuation of a share-in-savings contract entered into under this section in a subsequent fiscal year, the contract shall be canceled or terminated. The costs of cancellation or termination may be paid out of—

''(A) appropriations available for the performance of the contract;

''(B) appropriations available for acquisition of the information

technology procured under the contract, and not otherwise obligated; or

''(C) funds subsequently appropriated for payments of costs of cancellation or termination, subject to the limitations in paragraph (3).

''(2) The amount payable in the event of cancellation or termination of a share-in-savings contract shall be negotiated with the contractor at the time the contract is entered into.

''(3)(A) Subject to subparagraph (B), the head of an executive agency may enter into share-in-savings contracts under this section in any given fiscal year even if funds are not made specifically available for the full costs of cancellation or termination of the contract if funds are available and sufficient to make payments with respect to the first fiscal year of the contract and the following conditions are met regarding the funding of cancellation and termination liability:

''(i) The amount of unfunded contingent liability for the contract does not exceed the lesser of—

''(I) 25 percent of the estimated costs of a cancellation or termination; or

''(II) $5,000,000.

''(ii) Unfunded contingent liability in excess of $1,000,000 has been approved by the Director of the Office of Management and Budget or the Director's designee.

''(B) The aggregate number of share-in-savings contracts that may be entered into under subparagraph (A) by all executive agencies to which this chapter applies in a fiscal year may not exceed

5 in each of fiscal years 2003, 2004, and 2005.
‘‘(c) DEFINITIONS.—In this section:
‘‘(1) The term ‘contractor’ means a private entity that enters into a contract with an agency.
‘‘(2) The term ‘savings’ means—
‘‘(A) monetary savings to an agency; or
‘‘(B) savings in time or other benefits realized by the agency, including enhanced revenues (other than enhanced revenues from the collection of fees, taxes, debts, claims, or other amounts owed the Federal Government).
‘‘(3) The term ‘share-in-savings contract’ means a contract under which—
‘‘(A) a contractor provides solutions for—
‘‘(i) improving the agency’s mission-related or administrative processes; or
‘‘(ii) accelerating the achievement of agency missions; and
‘‘(B) the head of the agency pays the contractor an amount equal to a portion of the savings derived by the agency from—
‘‘(i) any improvements in mission-related or administrative processes that result from implementation of the solution; or
‘‘(ii) acceleration of achievement of agency missions.
‘‘(d) TERMINATION.—No share-in-savings contracts may be entered into under this section after September 30, 2005.’’.
(c) DEVELOPMENT OF INCENTIVES.—The Director of the Office of Management and Budget shall, in consultation with the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, and executive

agencies, develop techniques to permit an executive agency to retain

a portion of the savings (after payment of the contractor's share of the savings) derived from share-in-savings contracts as funds are appropriated to the agency in future fiscal years.

(d) REGULATIONS.—Not later than 270 days after the date of the enactment of this Act, the Federal Acquisition Regulation shall be revised to implement the provisions enacted by this section. Such revisions shall—

(1) provide for the use of competitive procedures in the selection and award of share-in-savings contracts to—

(A) ensure the contractor's share of savings reflects the risk involved and market conditions; and

(B) otherwise yield greatest value to the government; and

(2) allow appropriate regulatory flexibility to facilitate the use of share-in-savings contracts by executive agencies, including the use of innovative provisions for technology refreshment and nonstandard Federal Acquisition Regulation contract clauses.

(e) ADDITIONAL GUIDANCE.—The Administrator of General Services shall—

(1) identify potential opportunities for the use of sharein-savings contracts; and

(2) in consultation with the Director of the Office of Management and Budget, provide guidance to executive agencies for determining mutually beneficial savings share ratios and baselines from which savings may be measured.

(f) OMB REPORT TO CONGRESS.—In consultation with executive agencies, the Director of the Office of Management and Budget shall, not later than 2 years after the date of the enactment of this Act, submit to Congress a report containing—
(1) a description of the number of share-in-savings contracts entered into by each executive agency under by this section and the amendments made by this section, and, for each contract identified—
(A) the information technology acquired;
(B) the total amount of payments made to the contractor; and
(C) the total amount of savings or other measurable benefits realized;
(2) a description of the ability of agencies to determine the baseline costs of a project against which savings can be measured; and
(3) any recommendations, as the Director deems appropriate, regarding additional changes in law that may be necessary to ensure effective use of share-in-savings contracts by executive agencies.
(g) GAO REPORT TO CONGRESS.—The Comptroller General shall, not later than 6 months after the report required under subsection (f) is submitted to Congress, conduct a review of that report and submit to Congress a report containing—
(1) the results of the review;
(2) an independent assessment by the Comptroller General of the effectiveness of the use of share-in-savings contracts in improving the mission-related and administrative processes of the executive agencies and the achievement of agency missions; and

Deadline.

Deadline.

Deadline.

(3) a recommendation on whether the authority to enter into share-in-savings contracts should be continued.

(h) REPEAL OF SHARE-IN-SAVINGS PILOT PROGRAM.—

(1) REPEAL.—Section 11521 of title 40, United States Code, is repealed.

(2) CONFORMING AMENDMENTS TO PILOT PROGRAM AUTHORITY.—

(A) Section 11501 of title 40, United States Code, is amended—

(i) in the section heading, by striking ''**PROGRAMS**'' and inserting ''**PROGRAM**'';

(ii) in subsection (a)(1), by striking ''conduct pilot programs'' and inserting ''conduct a pilot program pursuant to the requirements of section 11521 of this title'';

(iii) in subsection (a)(2), by striking ''each pilot program'' and inserting ''the pilot program'';

(iv) in subsection (b), by striking ''LIMITATIONS.— '' and all that follows through ''$750,000,000.'' and inserting the following: ''LIMITATION ON AMOUNT.—The total amount obligated for contracts entered into under the pilot program conducted under this chapter may not exceed $375,000,000.''; and

(v) in subsection (c)(1), by striking ''a pilot'' and

inserting ‘‘the pilot’’.

(B) The following provisions of chapter 115 of such title are each amended by striking ‘‘a pilot’’ each place it appears and inserting ‘‘the pilot’’:

(i) Section 11502(a).

(ii) Section 11502(b).

(iii) Section 11503(a).

(iv) Section 11504.

(C) Section 11505 of such chapter is amended by striking ‘‘programs’’ and inserting ‘‘program’’.

(3) ADDITIONAL CONFORMING AMENDMENTS.—

(A) Section 11522 of title 40, United States Code, is redesignated as section 11521.

(B) The chapter heading for chapter 115 of such title is amended by striking ‘‘**PROGRAMS**’’ and inserting ‘‘**PROGRAM**’’.

(C) The subchapter heading for subchapter I and for subchapter II of such chapter are each amended by striking ‘‘PROGRAMS’’ and inserting ‘‘PROGRAM’’.

(D) The item relating to subchapter I in the table of sections at the beginning of such chapter is amended to read as follows:

‘‘SUBCHAPTER I—CONDUCT OF PILOT PROGRAM’’.

(E) The item relating to subchapter II in the table of sections at the beginning of such chapter is amended to read as follows:

‘‘SUBCHAPTER II—SPECIFIC PILOT PROGRAM’’.

(F) The item relating to section 11501 in the table of sections at the beginning of such is amended by striking ‘‘programs’’ and inserting ‘‘program’’.

(G) The table of sections at the beginning of such chapter is amended by striking the item relating to section 11521 and redesignating the item relating to section 11522 as section 11521.

(H) The item relating to chapter 115 in the table of chapters for subtitle III of title 40, United States Code, is amended to read as follows:

''115. INFORMATION TECHNOLOGY ACQUISITION PILOT PROGRAM ....11501''.

(i) DEFINITIONS.—In this section, the terms ''contractor'', ''savings'', and ''share-in-savings contract'' have the meanings given those terms in section 317 of the Federal Property and Administrative Services Act of 1949 (as added by subsection (b)).

SEC. 211. AUTHORIZATION FOR ACQUISITION OF INFORMATION TECHNOLOGY BY STATE AND LOCAL GOVERNMENTS THROUGH FEDERAL SUPPLY SCHEDULES.

(a) AUTHORITY TO USE CERTAIN SUPPLY SCHEDULES.—Section 502 of title 40, United States Code, is amended by adding at the end the following new subsection:

''(c) USE OF CERTAIN SUPPLY SCHEDULES.—

''(1) IN GENERAL.—The Administrator may provide for the use by State or local governments of Federal supply schedules of the General Services Administration for automated data processing equipment (including firmware), software, supplies, support equipment, and services (as contained in Federal supply classification code group 70).

''(2) VOLUNTARY USE.—In any case of the use by a State or local government of a Federal supply schedule pursuant

to paragraph (1), participation by a firm that sells to the Federal Government through the supply schedule shall be voluntary with respect to a sale to the State or local government through such supply schedule.

''(3) DEFINITIONS.—In this subsection:

''(A) The term 'State or local government' includes any State, local, regional, or tribal government, or any instrumentality thereof (including any local educational agency or institution of higher education).

''(B) The term 'tribal government' means—

''(i) the governing body of any Indian tribe, band, nation, or other organized group or community located in the continental United States (excluding the State of Alaska) that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians, and

''(ii) any Alaska Native regional or village corporation established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.).

''(C) The term 'local educational agency' has the meaning given that term in section 8013 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7713).

''(D) The term 'institution of higher education' has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).''.

(b) PROCEDURES.—Not later than 30 days after the date of the enactment of this Act, the Administrator of General Services shall establish procedures to implement section 501(c) of title 40, United States Code (as added by subsection (a)).

Deadline.

44 USC 3501 note.

(c) REPORT.—Not later than December 31, 2004, the Administrator shall submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a report on the implementation and effects of the amendment made by subsection (a).

SEC. 212. INTEGRATED REPORTING STUDY AND PILOT PROJECTS.

(a) PURPOSES.—The purposes of this section are to—

(1) enhance the interoperability of Federal information systems;

(2) assist the public, including the regulated community, in electronically submitting information to agencies under Federal requirements, by reducing the burden of duplicate collection and ensuring the accuracy of submitted information; and

(3) enable any person to integrate and obtain similar information held by 1 or more agencies under 1 or more Federal requirements without violating the privacy rights of an individual.

(b) DEFINITIONS.—In this section, the term—

(1) ''agency'' means an Executive agency as defined under section 105 of title 5, United States Code; and

(2) ''person'' means any individual, trust, firm, joint stock company, corporation (including a government corporation), partnership, association, State, municipality, commission, political subdivision of a State, interstate body, or agency or component of the Federal Government.

(c) REPORT.—

(1) IN GENERAL.—Not later than 3 years after the date

of enactment of this Act, the Director shall oversee a study, in consultation with agencies, the regulated community, public interest organizations, and the public, and submit a report to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives on progress toward integrating Federal information systems across agencies.

(2) CONTENTS.—The report under this section shall—

(A) address the integration of data elements used in the electronic collection of information within databases established under Federal statute without reducing the quality, accessibility, scope, or utility of the information contained in each database;

(B) address the feasibility of developing, or enabling the development of, software, including Internet-based tools, for use by reporting persons in assembling, documenting, and validating the accuracy of information electronically submitted to agencies under nonvoluntary, statutory, and regulatory requirements;

(C) address the feasibility of developing a distributed information system involving, on a voluntary basis, at least 2 agencies, that—

(i) provides consistent, dependable, and timely public access to the information holdings of 1 or more agencies, or some portion of such holdings, without requiring public users to know which agency holds the information; and

(ii) allows the integration of public information held by the participating agencies;

Deadline.

44 USC 3501 note.

Deadline.

(D) address the feasibility of incorporating other elements related to the purposes of this section at the discretion of the Director; and

(E) make any recommendations that the Director deems appropriate on the use of integrated reporting and information systems, to reduce the burden on reporting and strengthen public access to databases within and across agencies.

(d) PILOT PROJECTS TO ENCOURAGE INTEGRATED COLLECTION AND MANAGEMENT OF DATA AND INTEROPERABILITY OF FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—In order to provide input to the study under subsection (c), the Director shall designate, in consultation with agencies, a series of no more than 5 pilot projects that integrate data elements. The Director shall consult with agencies, the regulated community, public interest organizations, and the public on the implementation of the pilot projects.

(2) GOALS OF PILOT PROJECTS.—

(A) IN GENERAL.—Each goal described under subparagraph (B) shall be addressed by at least 1 pilot project each.

(B) GOALS.—The goals under this paragraph are to—

(i) reduce information collection burdens by eliminating duplicative data elements within 2 or more

reporting requirements;
(ii) create interoperability between or among public databases managed by 2 or more agencies using technologies and techniques that facilitate public access;
and
(iii) develop, or enable the development of, software to reduce errors in electronically submitted information.
(3) INPUT.—Each pilot project shall seek input from users on the utility of the pilot project and areas for improvement. To the extent practicable, the Director shall consult with relevant agencies and State, tribal, and local governments in carrying out the report and pilot projects under this section.
(e) PROTECTIONS.—The activities authorized under this section shall afford protections for—
(1) confidential business information consistent with section 552(b)(4) of title 5, United States Code, and other relevant law;
(2) personal privacy information under sections 552(b) (6) and (7)(C) and 552a of title 5, United States Code, and other relevant law;
(3) other information consistent with section 552(b)(3) of title 5, United States Code, and other relevant law; and
(4) confidential statistical information collected under a confidentiality pledge, solely for statistical purposes, consistent with the Office of Management and Budget's Federal Statistical Confidentiality Order, and other relevant law.

SEC. 213. COMMUNITY TECHNOLOGY CENTERS.

(a) PURPOSES.—The purposes of this section are to—
(1) study and enhance the effectiveness of community technology centers, public libraries, and other institutions that provide

computer and Internet access to the public; and

44 USC 3501 note.

(2) promote awareness of the availability of on-line government information and services, to users of community technology centers, public libraries, and other public facilities that provide access to computer technology and Internet access to the public.

(b) STUDY AND REPORT.—Not later than 2 years after the effective date of this title, the Administrator shall—

(1) ensure that a study is conducted to evaluate the best practices of community technology centers that have received Federal funds; and

(2) submit a report on the study to—

(A) the Committee on Governmental Affairs of the Senate;

(B) the Committee on Health, Education, Labor, and Pensions of the Senate;

(C) the Committee on Government Reform of the House of Representatives; and

(D) the Committee on Education and the Workforce of the House of Representatives.

(c) CONTENTS.—The report under subsection (b) may consider—

(1) an evaluation of the best practices being used by successful community technology centers;

(2) a strategy for—

(A) continuing the evaluation of best practices used

by community technology centers; and
(B) establishing a network to share information and resources as community technology centers evolve;
(3) the identification of methods to expand the use of best practices to assist community technology centers, public libraries, and other institutions that provide computer and Internet access to the public;
(4) a database of all community technology centers that have received Federal funds, including—
(A) each center's name, location, services provided, director, other points of contact, number of individuals served; and
(B) other relevant information;
(5) an analysis of whether community technology centers have been deployed effectively in urban and rural areas throughout the Nation; and
(6) recommendations of how to—
(A) enhance the development of community technology centers; and
(B) establish a network to share information and resources.
(d) COOPERATION.—All agencies that fund community technology centers shall provide to the Administrator any information and assistance necessary for the completion of the study and the report under this section.
(e) ASSISTANCE.—
(1) IN GENERAL.—The Administrator, in consultation with the Secretary of Education, shall work with other relevant Federal agencies, and other interested persons in the private and nonprofit sectors to—

(A) assist in the implementation of recommendations; and

Deadline.

(B) identify other ways to assist community technology centers, public libraries, and other institutions that provide computer and Internet access to the public.

(2) TYPES OF ASSISTANCE.—Assistance under this subsection may include—

(A) contribution of funds;

(B) donations of equipment, and training in the use and maintenance of the equipment; and

(C) the provision of basic instruction or training material in computer skills and Internet usage.

(f) ONLINE TUTORIAL.—

(1) IN GENERAL.—The Administrator, in consultation with the Secretary of Education, the Director of the Institute of Museum and Library Services, other relevant agencies, and the public, shall develop an online tutorial that—

(A) explains how to access Government information and services on the Internet; and

(B) provides a guide to available online resources.

(2) DISTRIBUTION.—The Administrator, with assistance from the Secretary of Education, shall distribute information on the tutorial to community technology centers, public libraries, and other institutions that afford Internet access to the public.

(g) PROMOTION OF COMMUNITY TECHNOLOGY CENTERS.—The

Administrator, with assistance from the Department of Education and in consultation with other agencies and organizations, shall promote the availability of community technology centers to raise awareness within each community where such a center is located.

(h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the study of best practices at community technology centers, for the development and dissemination of the online tutorial, and for the promotion of community technology centers under this section—

(1) $2,000,000 in fiscal year 2003;

(2) $2,000,000 in fiscal year 2004; and

(3) such sums as are necessary in fiscal years 2005 through 2007.

SEC. 214. ENHANCING CRISIS MANAGEMENT THROUGH ADVANCED INFORMATION TECHNOLOGY.

(a) PURPOSE.—The purpose of this section is to improve how information technology is used in coordinating and facilitating information on disaster preparedness, response, and recovery, while ensuring the availability of such information across multiple access channels.

(b) IN GENERAL.—

(1) STUDY ON ENHANCEMENT OF CRISIS RESPONSE.—Not later than 90 days after the date of enactment of this Act, the Administrator, in consultation with the Federal Emergency Management Agency, shall ensure that a study is conducted on using information technology to enhance crisis preparedness, response, and consequence management of natural and manmade disasters.

(2) CONTENTS.—The study under this subsection shall address—

(A) a research and implementation strategy for effective use of information technology in crisis response and

Deadline.

44 USC 3501 note.

consequence management, including the more effective use of technologies, management of information technology research initiatives, and incorporation of research advances into the information and communications systems of—

(i) the Federal Emergency Management Agency; and

(ii) other Federal, State, and local agencies responsible for crisis preparedness, response, and consequence management; and

(B) opportunities for research and development on enhanced technologies into areas of potential improvement as determined during the course of the study.

(3) REPORT.—Not later than 2 years after the date on which a contract is entered into under paragraph (1), the Administrator shall submit a report on the study, including findings and recommendations to—

(A) the Committee on Governmental Affairs of the Senate; and

(B) the Committee on Government Reform of the House of Representatives.

(4) INTERAGENCY COOPERATION.—Other Federal departments and agencies with responsibility for disaster relief and

emergency assistance shall fully cooperate with the Administrator in carrying out this section.

(5) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for research under this subsection, such sums as are necessary for fiscal year 2003.

(c) PILOT PROJECTS.—Based on the results of the research conducted under subsection (b), the Administrator, in consultation with the Federal Emergency Management Agency, shall initiate pilot projects or report to Congress on other activities that further the goal of maximizing the utility of information technology in disaster management. The Administrator shall cooperate with other relevant agencies, and, if appropriate, State, local, and tribal governments, in initiating such pilot projects.

SEC. 215. DISPARITIES IN ACCESS TO THE INTERNET.

(a) STUDY AND REPORT.—

(1) STUDY.—Not later than 90 days after the date of enactment of this Act, the Administrator of General Services shall request that the National Academy of Sciences, acting through the National Research Council, enter into a contract to conduct a study on disparities in Internet access for online Government services.

(2) REPORT.—Not later than 2 years after the date of enactment of this Act, the Administrator of General Services shall submit to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives a final report of the study under this section, which shall set forth the findings, conclusions, and recommendations of the National Research Council.

(b) CONTENTS.—The report under subsection (a) shall include a study of—

(1) how disparities in Internet access influence the effectiveness of online Government services, including a review of—

(A) the nature of disparities in Internet access;

(B) the affordability of Internet service;

Deadlines.

44 USC 3501 note.

Deadline.

(C) the incidence of disparities among different groups within the population; and

(D) changes in the nature of personal and public Internet access that may alleviate or aggravate effective access to online Government services;

(2) how the increase in online Government services is influencing the disparities in Internet access and how technology development or diffusion trends may offset such adverse influences; and

(3) related societal effects arising from the interplay of disparities in Internet access and the increase in online Government services.

(c) RECOMMENDATIONS.—The report shall include recommendations on actions to ensure that online Government initiatives shall not have the unintended result of increasing any deficiency in public access to Government services.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $950,000 in fiscal year 2003 to carry out this section.

SEC. 216. COMMON PROTOCOLS FOR GEOGRAPHIC INFORMATION SYSTEMS.

(a) PURPOSES.—The purposes of this section are to—

(1) reduce redundant data collection and information; and

(2) promote collaboration and use of standards for government geographic information.

(b) DEFINITION.—In this section, the term ‘‘geographic information’’ means information systems that involve locational data, such as maps or other geospatial information resources.

(c) IN GENERAL.—

(1) COMMON PROTOCOLS.—The Administrator, in consultation with the Secretary of the Interior, working with the Director and through an interagency group, and working with private sector experts, State, local, and tribal governments, commercial and international standards groups, and other interested parties, shall facilitate the development of common protocols for the development, acquisition, maintenance, distribution, and application of geographic information. If practicable, the Administrator shall incorporate intergovernmental and public private geographic information partnerships into efforts under this subsection.

(2) INTERAGENCY GROUP.—The interagency group referred to under paragraph (1) shall include representatives of the National Institute of Standards and Technology and other agencies.

(d) DIRECTOR.—The Director shall oversee—

(1) the interagency initiative to develop common protocols;

(2) the coordination with State, local, and tribal governments, public private partnerships, and other interested persons on effective and efficient ways to align geographic information and develop common protocols; and

(3) the adoption of common standards relating to the protocols.

(e) COMMON PROTOCOLS.—The common protocols shall be designed to—

44 USC 3501 note.

(1) maximize the degree to which unclassified geographic information from various sources can be made electronically compatible and accessible; and

(2) promote the development of interoperable geographic information systems technologies that shall—

(A) allow widespread, low-cost use and sharing of geographic data by Federal agencies, State, local, and tribal governments, and the public; and

(B) enable the enhancement of services using geographic data.

(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are necessary to carry out this section, for each of the fiscal years 2003 through 2007.

TITLE III—INFORMATION SECURITY

SEC. 301. INFORMATION SECURITY.

(a) SHORT TITLE.—This title may be cited as the ''Federal Information Security Management Act of 2002''.

(b) INFORMATION SECURITY.—

(1) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter:

''SUBCHAPTER III—INFORMATION SECURITY

''§ 3541. Purposes

‘‘The purposes of this subchapter are to—
‘‘(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;
‘‘(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;
‘‘(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;
‘‘(4) provide a mechanism for improved oversight of Federal agency information security programs;
‘‘(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and
‘‘(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

44 USC 101 note.

Federal Information Security

Management

Act of 2002.

‘‘§ 3542. Definitions

‘‘(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

‘‘(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

‘‘(1) The term ‘information security’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

‘‘(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

‘‘(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

‘‘(C) availability, which means ensuring timely and reliable access to and use of information.

‘‘(2)(A) The term ‘national security system’ means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

‘‘(i) the function, operation, or use of which—

‘‘(I) involves intelligence activities;

‘‘(II) involves cryptologic activities related to national security;

‘‘(III) involves command and control of military
forces;
‘‘(IV) involves equipment that is an integral part
of a weapon or weapons system; or
‘‘(V) subject to subparagraph (B), is critical to the
direct fulfillment of military or intelligence missions;
or
‘‘(ii) is protected at all times by procedures established
for information that have been specifically authorized under
criteria established by an Executive order or an Act of
Congress to be kept classified in the interest of national
defense or foreign policy.
‘‘(B) Subparagraph (A)(i)(V) does not include a system that
is to be used for routine administrative and business applications
(including payroll, finance, logistics, and personnel
management applications).
‘‘(3) The term ‘information technology’ has the meaning
given that term in section 11101 of title 40.
‘‘§ 3543. Authority and functions of the Director
‘‘(a) IN GENERAL.—The Director shall oversee agency information
security policies and practices, including—
‘‘(1) developing and overseeing the implementation of policies,
principles, standards, and guidelines on information security,
including through ensuring timely agency adoption of and
compliance with standards promulgated under section 11331
of title 40;
‘‘(2) requiring agencies, consistent with the standards
promulgated under such section 11331 and the requirements
of this subchapter, to identify and provide information security
protections commensurate with the risk and magnitude of the

harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

''(A) information collected or maintained by or on behalf of an agency; or

''(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

''(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

''(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

''(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3544(b);

''(6) coordinating information security policies and procedures with related information resources management policies and procedures;

''(7) overseeing the operation of the Federal information security incident center required under section 3546; and

‘‘(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

‘‘(A) a summary of the findings of evaluations required by section 3545;

‘‘(B) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under section 11331 of title 40;

‘‘(C) significant deficiencies in agency information security practices;

‘‘(D) planned remedial action to address such deficiencies; and

‘‘(E) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

‘‘(b) NATIONAL SECURITY SYSTEMS.—Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

‘‘(c) DEPARTMENT OF DEFENSE AND CENTRAL INTELLIGENCE AGENCY SYSTEMS.—(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3).

‘‘(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

‘‘(3) The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

‘‘§ 3544. Federal agency responsibilities

‘‘(a) IN GENERAL.—The head of each agency shall—

‘‘(1) be responsible for—

‘‘(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

‘‘(i) information collected or maintained by or on behalf of the agency; and

‘‘(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

‘‘(B) complying with the requirements of this subchapter and related policies, procedures, standards, and

guidelines, including—
‘‘(i) information security standards promulgated
under section 11331 of title 40; and
‘‘(ii) information security standards and guidelines
for national security systems issued in accordance with
law and as directed by the President; and
‘‘(C) ensuring that information security management
processes are integrated with agency strategic and operational
planning processes;
‘‘(2) ensure that senior agency officials provide information
security for the information and information systems that support
the operations and assets under their control, including
through—
‘‘(A) assessing the risk and magnitude of the harm
that could result from the unauthorized access, use, disclosure,
disruption, modification, or destruction of such
information or information systems;
‘‘(B) determining the levels of information security
appropriate to protect such information and information
systems in accordance with standards promulgated under
section 11331 of title 40, for information security classifications
and related requirements;
‘‘(C) implementing policies and procedures to cost-effectively
reduce risks to an acceptable level; and
‘‘(D) periodically testing and evaluating information
security controls and techniques to ensure that they are
effectively implemented;

‘‘(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

‘‘(A) designating a senior agency information security officer who shall—

‘‘(i) carry out the Chief Information Officer’s responsibilities under this section;

‘‘(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

‘‘(iii) have information security duties as that official’s primary duty; and

‘‘(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

‘‘(B) developing and maintaining an agencywide information security program as required by subsection (b);

‘‘(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3543 of this title, and section 11331 of title 40;

‘‘(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

‘‘(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

‘‘(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of

this subchapter and related policies, procedures, standards,
and guidelines; and
‘‘(5) ensure that the agency Chief Information Officer, in
coordination with other senior agency officials, reports annually
to the agency head on the effectiveness of the agency information
security program, including progress of remedial actions.
‘‘(b) AGENCY PROGRAM.—Each agency shall develop, document,
and implement an agencywide information security program,
approved by the Director under section 3543(a)(5), to provide
information security for the information and information systems
that support the operations and assets of the agency, including
those provided or managed by another agency, contractor, or other
source, that includes—
‘‘(1) periodic assessments of the risk and magnitude of
the harm that could result from the unauthorized access, use,
disclosure, disruption, modification, or destruction of information
and information systems that support the operations and
assets of the agency;
‘‘(2) policies and procedures that—
‘‘(A) are based on the risk assessments required by
paragraph (1);
‘‘(B) cost-effectively reduce information security risks
to an acceptable level;
‘‘(C) ensure that information security is addressed
throughout the life cycle of each agency information system;
and

‘‘(D) ensure compliance with—

‘‘(i) the requirements of this subchapter;
‘‘(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;
‘‘(iii) minimally acceptable system configuration requirements, as determined by the agency; and
‘‘(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;
‘‘(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
‘‘(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—
‘‘(A) information security risks associated with their activities; and
‘‘(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;
‘‘(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—
‘‘(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and
‘‘(B) may include testing relied on in a evaluation under section 3545;
‘‘(6) a process for planning, implementing, evaluating, and

documenting remedial action to address any deficiencies in
the information security policies, procedures, and practices of
the agency;
‘‘(7) procedures for detecting, reporting, and responding
to security incidents, consistent with standards and guidelines
issued pursuant to section 3546(b), including—
‘‘(A) mitigating risks associated with such incidents
before substantial damage is done;
‘‘(B) notifying and consulting with the Federal information
security incident center referred to in section 3546;
and
‘‘(C) notifying and consulting with, as appropriate—
‘‘(i) law enforcement agencies and relevant Offices
of Inspector General;
‘‘(ii) an office designated by the President for any
incident involving a national security system; and
‘‘(iii) any other agency or office, in accordance with
law or as directed by the President; and
‘‘(8) plans and procedures to ensure continuity of operations
for information systems that support the operations and assets
of the agency.
‘‘(c) AGENCY REPORTING.—Each agency shall—
‘‘(1) report annually to the Director, the Committees on
Government Reform and Science of the House of Representatives,
the Committees on Governmental Affairs and Commerce,
Science, and Transportation of the Senate, the appropriate

authorization and appropriations committees of Congress, and

the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

‘‘(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

‘‘(A) annual agency budgets;

‘‘(B) information resources management under subchapter 1 of this chapter;

‘‘(C) information technology management under subtitle III of title 40;

‘‘(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

‘‘(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

‘‘(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

‘‘(G) internal accounting and administrative controls under section 3512 of title 31, (known as the ‘Federal Managers Financial Integrity Act’); and

‘‘(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

‘‘(A) as a material weakness in reporting under section 3512 of title 31; and

‘‘(B) if relating to financial management systems, as

an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

''(d) PERFORMANCE PLAN.—(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

''(A) the time periods, and

''(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

''(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

''(e) PUBLIC NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

''§ 3545. Annual independent evaluation

''(a) IN GENERAL.—(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

''(2) Each evaluation under this section shall include—

''(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

‘‘(B) an assessment (made on the basis of the results of the testing) of compliance with—

‘‘(i) the requirements of this subchapter; and

‘‘(ii) related information security policies, procedures, standards, and guidelines; and

‘‘(C) separate presentations, as appropriate, regarding information security relating to national security systems.

‘‘(b) INDEPENDENT AUDITOR.—Subject to subsection (c)—

‘‘(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

‘‘(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

‘‘(c) NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

‘‘(1) only by an entity designated by the agency head; and

‘‘(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

‘‘(d) EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

‘‘(e) AGENCY REPORTING.—(1) Each year, not later than such

date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

''(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

''(f) PROTECTION OF INFORMATION.—Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

''(g) OMB REPORTS TO CONGRESS.—(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3543(a)(8).

''(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

''(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central

Deadline.

Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall

be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

''(h) COMPTROLLER GENERAL.—The Comptroller General shall periodically evaluate and report to Congress on—

''(1) the adequacy and effectiveness of agency information security policies and practices; and

''(2) implementation of the requirements of this subchapter.

''§ 3546. Federal information security incident center

''(a) IN GENERAL.—The Director shall ensure the operation of a central Federal information security incident center to—

''(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

''(2) compile and analyze information about incidents that threaten information security;

''(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

''(4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

''(b) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national

security systems, issued in accordance with law and as directed by the President.

‘‘§ 3547. National security systems

‘‘The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

‘‘(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

‘‘(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

‘‘(3) complies with the requirements of this subchapter.

‘‘§ 3548. Authorization of appropriations

‘‘There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

Reports.

‘‘§ 3549. Effect on existing law

‘‘Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure

of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States. While this subchapter is in effect, subchapter II of this chapter shall not apply.''.

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter 35 is amended by adding at the end the following:

''SUBCHAPTER III—INFORMATION SECURITY

''Sec.

''3541. Purposes.

''3542. Definitions.

''3543. Authority and functions of the Director.

''3544. Federal agency responsibilities.

''3545. Annual independent evaluation.

''3546. Federal information security incident center.

''3547. National security systems.

''3548. Authorization of appropriations.

''3549. Effect on existing law.''.

(c) INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES.—

(1) NATIONAL SECURITY RESPONSIBILITIES.—(A) Nothing in this Act (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by section 3542(b)(2) of title 44, United

States Code.

(B) Section 2224 of title 10, United States Code, is amended—

(i) in subsection (b), by striking ‘‘(b) OBJECTIVES AND MINIMUM REQUIREMENTS.—(1)’’ and inserting ‘‘(b) OBJECTIVES OF THE PROGRAM.—’’;

(ii) in subsection (b), by striking paragraph (2); and

(iii) in subsection (c), in the matter preceding paragraph (1), by inserting ‘‘, including through compliance with subchapter III of chapter 35 of title 44’’ after ‘‘infrastructure’’.

(2) ATOMIC ENERGY ACT OF 1954.—Nothing in this Act shall supersede any requirement made by or under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted data or formerly restricted data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

44 USC 3501 note.

44 USC 3501 note.

SEC. 302. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

‘‘§ 11331. Responsibilities for Federal information systems standards

‘‘(a) STANDARDS AND GUIDELINES.—

‘‘(1) AUTHORITY TO PRESCRIBE.—Except as provided under

paragraph (2), the Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), prescribe standards and guidelines pertaining to Federal information systems.

''(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems (as defined under this section) shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.

''(b) MANDATORY REQUIREMENTS.—

''(1) AUTHORITY TO MAKE MANDATORY.—Except as provided under paragraph (2), the Secretary shall make standards prescribed under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of Federal information systems.

''(2) REQUIRED MANDATORY STANDARDS.—(A) Standards prescribed under subsection (a)(1) shall include information security standards that—

''(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)); and

''(ii) are otherwise necessary to improve the security of Federal information and information systems.

''(B) Information security standards described in subparagraph (A) shall be compulsory and binding.

''(c) AUTHORITY TO DISAPPROVE OR MODIFY.—The President may disapprove or modify the standards and guidelines referred to in subsection (a)(1) if the President determines such action to be

in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

''(d) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget.

''(e) APPLICATION OF MORE STRINGENT STANDARDS.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Secretary prescribes under this section if the more stringent standards—

Federal Register, publication.

PUBLIC LAW 107–347—DEC. 17 2002 116 STAT. 2957

''(1) contain at least the applicable standards made compulsory and binding by the Secretary; and

''(2) are otherwise consistent with policies and guidelines issued under section 3543 of title 44.

''(f) DECISIONS ON PROMULGATION OF STANDARDS.—The decision by the Secretary regarding the promulgation of any standard under this section shall occur not later than 6 months after the submission of the proposed standard to the Secretary by the National Institute

of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

''(g) DEFINITIONS.—In this section:

''(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

''(2) INFORMATION SECURITY.—The term 'information security' has the meaning given that term in section 3542(b)(1) of title 44.

''(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given that term in section 3542(b)(2) of title 44.''.

(b) CLERICAL AMENDMENT.—The item relating to section 11331 in the table of sections at the beginning of chapter 113 of such title is amended to read as follows:

''11331. Responsibilities for Federal information systems standards.''.

SEC. 303. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), is amended by striking the text and inserting the following:

''(a) IN GENERAL.—The Institute shall—

''(1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

''(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems

(as defined in section 3542(b)(2) of title 44, United States Code); and

''(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

''(b) MINIMUM REQUIREMENTS FOR STANDARDS AND GUIDELINES.—The standards and guidelines required by subsection (a) shall include, at a minimum—

''(1)(A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;

''(B) guidelines recommending the types of information and information systems to be included in each such category; and

Deadline.

''(C) minimum information security requirements for information and information systems in each such category;

''(2) a definition of and guidelines concerning detection and handling of information security incidents; and

''(3) guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system consistent with applicable requirements for national security systems, issued in accordance with law and as directed by the President.

‘‘(c) DEVELOPMENT OF STANDARDS AND GUIDELINES.—In developing standards and guidelines required by subsections (a) and (b), the Institute shall—

‘‘(1) consult with other agencies and offices and the private sector (including the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security) to assure—

‘‘(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid unnecessary and costly duplication of effort; and

‘‘(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

‘‘(2) provide the public with an opportunity to comment on proposed standards and guidelines;

‘‘(3) submit to the Secretary of Commerce for promulgation under section 11331 of title 40, United States Code—

‘‘(A) standards, as required under subsection (b)(1)(A), no later than 12 months after the date of the enactment of this section; and

‘‘(B) minimum information security requirements for each category, as required under subsection (b)(1)(C), no later than 36 months after the date of the enactment of this section;

‘‘(4) issue guidelines as required under subsection (b)(1)(B), no later than 18 months after the date of the enactment of this section;

‘‘(5) to the maximum extent practicable, ensure that such standards and guidelines do not require the use or procurement of specific products, including any specific hardware or software;

‘‘(6) to the maximum extent practicable, ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and

‘‘(7) to the maximum extent practicable, use flexible, performance-based standards and guidelines that permit the use of off-the-shelf commercially developed information security products.

‘‘(d) INFORMATION SECURITY FUNCTIONS.—The Institute shall—

‘‘(1) submit standards developed pursuant to subsection (a), along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 11331 of title 40, United States Code;

Deadline.

Deadlines.

‘‘(2) provide technical assistance to agencies, upon request, regarding—

‘‘(A) compliance with the standards and guidelines developed under subsection (a);

‘‘(B) detecting and handling information security incidents; and

‘‘(C) information security policies, procedures, and practices;

‘‘(3) conduct research, as needed, to determine the nature

and extent of information security vulnerabilities and techniques
for providing cost-effective information security;
‘‘(4) develop and periodically revise performance indicators
and measures for agency information security policies and practices;
‘‘(5) evaluate private sector information security policies
and practices and commercially available information technologies
to assess potential application by agencies to
strengthen information security;
‘‘(6) assist the private sector, upon request, in using and
applying the results of activities under this section;
‘‘(7) evaluate security policies and practices developed for
national security systems to assess potential application by
agencies to strengthen information security;
‘‘(8) periodically assess the effectiveness of standards and
guidelines developed under this section and undertake revisions
as appropriate;
‘‘(9) solicit and consider the recommendations of the
Information Security and Privacy Advisory Board, established
by section 21, regarding standards and guidelines developed
under subsection (a) and submit such recommendations to the
Secretary of Commerce with such standards submitted to the
Secretary; and
‘‘(10) prepare an annual public report on activities undertaken
in the previous year, and planned for the coming year,
to carry out responsibilities under this section.
‘‘(e) DEFINITIONS.—As used in this section—
‘‘(1) the term ‘agency’ has the same meaning as provided
in section 3502(1) of title 44, United States Code;
‘‘(2) the term ‘information security’ has the same meaning
as provided in section 3542(b)(1) of such title;

‘‘(3) the term ‘information system’ has the same meaning as provided in section 3502(8) of such title;
‘‘(4) the term ‘information technology’ has the same meaning as provided in section 11101 of title 40, United States Code; and
‘‘(5) the term ‘national security system’ has the same meaning as provided in section 3542(b)(2) of title 44, United States Code.
‘‘(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Commerce $20,000,000 for each of fiscal years 2003, 2004, 2005, 2006, and 2007 to enable the National Institute of Standards and Technology to carry out the provisions of this section.’’.

SEC. 304. INFORMATION SECURITY AND PRIVACY ADVISORY BOARD.

Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4), is amended—

116 STAT. 2960 PUBLIC LAW 107–347—DEC. 17 2002

(1) in subsection (a), by striking ‘‘Computer System Security and Privacy Advisory Board’’ and inserting ‘‘Information Security and Privacy Advisory Board’’;
(2) in subsection (a)(1), by striking ‘‘computer or telecommunications’’ and inserting ‘‘information technology’’;
(3) in subsection (a)(2)—
(A) by striking ‘‘computer or telecommunications technology’’ and inserting ‘‘information technology’’; and
(B) by striking ‘‘computer or telecommunications equipment’’ and inserting ‘‘information technology’’;
(4) in subsection (a)(3)—

(A) by striking ‘‘computer systems’’ and inserting
‘‘information system’’; and
(B) by striking ‘‘computer systems security’’ and
inserting ‘‘information security’’;
(5) in subsection (b)(1) by striking ‘‘computer systems security’’
and inserting ‘‘information security’’;
(6) in subsection (b) by striking paragraph (2) and inserting
the following:
‘‘(2) to advise the Institute, the Secretary of Commerce,
and the Director of the Office of Management and Budget
on information security and privacy issues pertaining to Federal
Government information systems, including through review of
proposed standards and guidelines developed under section 20;
and’’;
(7) in subsection (b)(3) by inserting ‘‘annually’’ after
‘‘report’’;
(8) by inserting after subsection (e) the following new subsection:
‘‘(f) The Board shall hold meetings at such locations and at
such time and place as determined by a majority of the Board.’’;
(9) by redesignating subsections (f) and (g) as subsections
(g) and (h), respectively; and
(10) by striking subsection (h), as redesignated by paragraph
(9), and inserting the following:
‘‘(h) As used in this section, the terms ‘information system’
and ‘information technology’ have the meanings given in section
20.’’.

SEC. 305. TECHNICAL AND CONFORMING AMENDMENTS.

(a) COMPUTER SECURITY ACT.—Section 11332 of title 40, United
States Code, and the item relating to that section in the table
of sections for chapter 113 of such title, are repealed.

(b) FLOYD D. SPENCE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2001.—The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Public Law 106–398) is amended by striking section 1062 (44 U.S.C. 3531 note).

(c) PAPERWORK REDUCTION ACT.—(1) Section 3504(g) of title 44, United States Code, is amended—

(A) by adding ''and'' at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking ''sections 11331 and 11332(b) and (c) of title 40'' and inserting ''section 11331 of title 40 and subchapter II of this chapter''; and

(ii) by striking ''; and'' and inserting a period; and

(C) by striking paragraph (3).

PUBLIC LAW 107–347—DEC. 17 2002 116 STAT. 2961

(2) Section 3505 of such title is amended by adding at the end—

''(c) INVENTORY OF MAJOR INFORMATION SYSTEMS.—(1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.

''(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.

''(3) Such inventory shall be—

''(A) updated at least annually;

''(B) made available to the Comptroller General; and

''(C) used to support information resources management,

including—

‘‘(i) preparation and maintenance of the inventory of information resources under section 3506(b)(4);

‘‘(ii) information technology planning, budgeting, acquisition, and management under section 3506(h), subtitle III of title 40, and related laws and guidance;

‘‘(iii) monitoring, testing, and evaluation of information security controls under subchapter II;

‘‘(iv) preparation of the index of major information systems required under section 552(g) of title 5, United States Code; and

‘‘(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33.

‘‘(4) The Director shall issue guidance for and oversee the implementation of the requirements of this subsection.’’.

(3) Section 3506(g) of such title is amended—

(A) by adding ‘‘and’’ at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking ‘‘section 11332 of title 40’’ and inserting ‘‘subchapter II of this chapter’’; and

(ii) by striking ‘‘; and’’ and inserting a period; and

(C) by striking paragraph (3).

TITLE IV—AUTHORIZATION OF APPROPRIATIONS AND EFFECTIVE DATES

SEC. 401. AUTHORIZATION OF APPROPRIATIONS.

Except for those purposes for which an authorization of appropriations is specifically provided in title I or II, including the amendments made by such titles, there are authorized to be appropriated such sums as are necessary to carry out titles I and II for each

of fiscal years 2003 through 2007.

SEC. 402. EFFECTIVE DATES.

(a) TITLES I AND II.—

(1) IN GENERAL.—Except as provided under paragraph (2), titles I and II and the amendments made by such titles shall take effect 120 days after the date of enactment of this Act.

(2) IMMEDIATE ENACTMENT.—Sections 207, 214, and 215 shall take effect on the date of enactment of this Act.

44 USC 3601 note.

(b) TITLES III AND IV.—Title III and this title shall take effect on the date of enactment of this Act.

TITLE V—CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY

SEC. 501. SHORT TITLE.

This title may be cited as the ‘‘Confidential Information Protection and Statistical Efficiency Act of 2002’’.

SEC. 502. DEFINITIONS.

As used in this title:

(1) The term ‘‘agency’’ means any entity that falls within the definition of the term ‘‘executive agency’’ as defined in section 102 of title 31, United States Code, or ‘‘agency’’, as defined in section 3502 of title 44, United States Code.

(2) The term ‘‘agent’’ means an individual—

(A)(i) who is an employee of a private organization or a researcher affiliated with an institution of higher learning (including a person granted special sworn status

by the Bureau of the Census under section 23(c) of title 13, United States Code), and with whom a contract or other agreement is executed, on a temporary basis, by an executive agency to perform exclusively statistical activities under the control and supervision of an officer or employee of that agency;

(ii) who is working under the authority of a government entity with which a contract or other agreement is executed by an executive agency to perform exclusively statistical activities under the control of an officer or employee of that agency;

(iii) who is a self-employed researcher, a consultant, a contractor, or an employee of a contractor, and with whom a contract or other agreement is executed by an executive agency to perform a statistical activity under the control of an officer or employee of that agency; or

(iv) who is a contractor or an employee of a contractor, and who is engaged by the agency to design or maintain the systems for handling or storage of data received under this title; and

(B) who agrees in writing to comply with all provisions of law that affect information acquired by that agency.

(3) The term ‘‘business data’’ means operating and financial data and information about businesses, tax-exempt organizations, and government entities.

(4) The term ‘‘identifiable form’’ means any representation of information that permits the identity of the respondent to whom the information applies to be reasonably inferred by either direct or indirect means.

(5) The term ‘‘nonstatistical purpose’’—

(A) means the use of data in identifiable form for any purpose that is not a statistical purpose, including

44 USC 3501 note.

44 USC 3501 note.

Confidential Information Protection and Statistical Efficiency Act of 2002.

44 USC 3541 note.

any administrative, regulatory, law enforcement, adjudicatory, or other purpose that affects the rights, privileges, or benefits of a particular identifiable respondent; and

(B) includes the disclosure under section 552 of title 5, United States Code (popularly known as the Freedom of Information Act) of data that are acquired for exclusively statistical purposes under a pledge of confidentiality.

(6) The term ‘‘respondent’’ means a person who, or organization that, is requested or required to supply information to an agency, is the subject of information requested or required to be supplied to an agency, or provides that information to an agency.

(7) The term ‘‘statistical activities’’—

(A) means the collection, compilation, processing, or analysis of data for the purpose of describing or making estimates concerning the whole, or relevant groups or components within, the economy, society, or the natural environment; and

(B) includes the development of methods or resources that support those activities, such as measurement methods, models, statistical classifications, or sampling frames.

(8) The term ''statistical agency or unit'' means an agency or organizational unit of the executive branch whose activities are predominantly the collection, compilation, processing, or analysis of information for statistical purposes.

(9) The term ''statistical purpose''—

(A) means the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; and

(B) includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support the purposes described in subparagraph (A).

SEC. 503. COORDINATION AND OVERSIGHT OF POLICIES.

(a) IN GENERAL.—The Director of the Office of Management and Budget shall coordinate and oversee the confidentiality and disclosure policies established by this title. The Director may promulgate rules or provide other guidance to ensure consistent interpretation of this title by the affected agencies.

(b) AGENCY RULES.—Subject to subsection (c), agencies may promulgate rules to implement this title. Rules governing disclosures

of information that are authorized by this title shall be promulgated by the agency that originally collected the information.

(c) REVIEW AND APPROVAL OF RULES.—The Director shall review any rules proposed by an agency pursuant to this title for consistency with the provisions of this title and chapter 35 of title 44, United States Code, and such rules shall be subject to the approval of the Director.

(d) REPORTS.—

(1) The head of each agency shall provide to the Director of the Office of Management and Budget such reports and other information as the Director requests.

(2) Each Designated Statistical Agency referred to in section 522 shall report annually to the Director of the Office

44 USC 3501 note.

of Management and Budget, the Committee on Government Reform of the House of Representatives, and the Committee on Governmental Affairs of the Senate on the actions it has taken to implement sections 523 and 524. The report shall include copies of each written agreement entered into pursuant to section 524(a) for the applicable year.

(3) The Director of the Office of Management and Budget shall include a summary of reports submitted to the Director under paragraph (2) and actions taken by the Director to advance the purposes of this title in the annual report to the Congress on statistical programs prepared under section 3504(e)(2) of title 44, United States Code.

SEC. 504. EFFECT ON OTHER LAWS.

(a) TITLE 44, UNITED STATES CODE.—This title, including amendments made by this title, does not diminish the authority under section 3510 of title 44, United States Code, of the Director of the Office of Management and Budget to direct, and of an agency to make, disclosures that are not inconsistent with any applicable law.

(b) TITLE 13 AND TITLE 44, UNITED STATES CODE.—This title, including amendments made by this title, does not diminish the authority of the Bureau of the Census to provide information in accordance with sections 8, 16, 301, and 401 of title 13, United States Code, and section 2108 of title 44, United States Code.

(c) TITLE 13, UNITED STATES CODE.—This title, including amendments made by this title, shall not be construed as authorizing the disclosure for nonstatistical purposes of demographic data or information collected by the Census Bureau pursuant to section 9 of title 13, United States Code.

(d) VARIOUS ENERGY STATUTES.—Data or information acquired by the Energy Information Administration under a pledge of confidentiality and designated by the Energy Information Administration to be used for exclusively statistical purposes shall not be disclosed in identifiable form for nonstatistical purposes under—

(1) section 12, 20, or 59 of the Federal Energy Administration Act of 1974 (15 U.S.C. 771, 779, 790h);

(2) section 11 of the Energy Supply and Environmental Coordination Act of 1974 (15 U.S.C. 796); or

(3) section 205 or 407 of the Department of the Energy Organization Act of 1977 (42 U.S.C. 7135, 7177).

(e) SECTION 201 OF CONGRESSIONAL BUDGET ACT OF 1974.—This title, including amendments made by this title, shall not

be construed to limit any authorities of the Congressional Budget Office to work (consistent with laws governing the confidentiality of information the disclosure of which would be a violation of law) with databases of Designated Statistical Agencies (as defined in section 522), either separately or, for data that may be shared pursuant to section 524 of this title or other authority, jointly in order to improve the general utility of these databases for the statistical purpose of analyzing pension and health care financing issues.

(f) PREEMPTION OF STATE LAW.—Nothing in this title shall preempt applicable State law regarding the confidentiality of data collected by the States.

44 USC 3501 note.

PUBLIC LAW 107–347—DEC. 17 2002 116 STAT. 2965

(g) STATUTES REGARDING FALSE STATEMENTS.—Notwithstanding section 512, information collected by an agency for exclusively statistical purposes under a pledge of confidentiality may be provided by the collecting agency to a law enforcement agency for the prosecution of submissions to the collecting agency of false statistical information under statutes that authorize criminal penalties (such as section 221 of title 13, United States Code) or civil penalties for the provision of false statistical information, unless such disclosure or use would otherwise be prohibited under Federal law.

(h) CONSTRUCTION.—Nothing in this title shall be construed as restricting or diminishing any confidentiality protections or penalties for unauthorized disclosure that otherwise apply to data

or information collected for statistical purposes or nonstatistical purposes, including, but not limited to, section 6103 of the Internal Revenue Code of 1986 (26 U.S.C. 6103).

(i) AUTHORITY OF CONGRESS.—Nothing in this title shall be construed to affect the authority of the Congress, including its committees, members, or agents, to obtain data or information for a statistical purpose, including for oversight of an agency's statistical activities.

Subtitle A—Confidential Information Protection

SEC. 511. FINDINGS AND PURPOSES.

(a) FINDINGS.—The Congress finds the following:

(1) Individuals, businesses, and other organizations have varying degrees of legal protection when providing information to the agencies for strictly statistical purposes.

(2) Pledges of confidentiality by agencies provide assurances to the public that information about individuals or organizations or provided by individuals or organizations for exclusively statistical purposes will be held in confidence and will not be used against such individuals or organizations in any agency action.

(3) Protecting the confidentiality interests of individuals or organizations who provide information under a pledge of confidentiality for Federal statistical programs serves both the interests of the public and the needs of society.

(4) Declining trust of the public in the protection of information provided under a pledge of confidentiality to the agencies adversely affects both the accuracy and completeness of statistical analyses.

(5) Ensuring that information provided under a pledge

of confidentiality for statistical purposes receives protection
is essential in continuing public cooperation in statistical programs.
(b) PURPOSES.—The purposes of this subtitle are the following:
(1) To ensure that information supplied by individuals or
organizations to an agency for statistical purposes under a
pledge of confidentiality is used exclusively for statistical purposes.
(2) To ensure that individuals or organizations who supply
information under a pledge of confidentiality to agencies for
statistical purposes will neither have that information disclosed
44 USC 3501
note.

in identifiable form to anyone not authorized by this title nor
have that information used for any purpose other than a statistical
purpose.
(3) To safeguard the confidentiality of individually identifiable
information acquired under a pledge of confidentiality
for statistical purposes by controlling access to, and uses made
of, such information.

SEC. 512. LIMITATIONS ON USE AND DISCLOSURE OF DATA AND INFORMATION.

(a) USE OF STATISTICAL DATA OR INFORMATION.—Data or
information acquired by an agency under a pledge of confidentiality
and for exclusively statistical purposes shall be used by officers,
employees, or agents of the agency exclusively for statistical purposes.
(b) DISCLOSURE OF STATISTICAL DATA OR INFORMATION.—
(1) Data or information acquired by an agency under a
pledge of confidentiality for exclusively statistical purposes shall

not be disclosed by an agency in identifiable form, for any use other than an exclusively statistical purpose, except with the informed consent of the respondent.

(2) A disclosure pursuant to paragraph (1) is authorized only when the head of the agency approves such disclosure and the disclosure is not prohibited by any other law.

(3) This section does not restrict or diminish any confidentiality protections in law that otherwise apply to data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes.

(c) RULE FOR USE OF DATA OR INFORMATION FOR NONSTATISTICAL PURPOSES.—A statistical agency or unit shall clearly distinguish any data or information it collects for nonstatistical purposes (as authorized by law) and provide notice to the public, before the data or information is collected, that the data or information could be used for nonstatistical purposes.

(d) DESIGNATION OF AGENTS.—A statistical agency or unit may designate agents, by contract or by entering into a special agreement containing the provisions required under section 502(2) for treatment as an agent under that section, who may perform exclusively statistical activities, subject to the limitations and penalties described in this title.

SEC. 513. FINES AND PENALTIES.

Whoever, being an officer, employee, or agent of an agency acquiring information for exclusively statistical purposes, having taken and subscribed the oath of office, or having sworn to observe the limitations imposed by section 512, comes into possession of such information by reason of his or her being an officer, employee, or agent and, knowing that the disclosure of the specific information is prohibited under the provisions of this title, willfully discloses

the information in any manner to a person or agency not entitled to receive it, shall be guilty of a class E felony and imprisoned for not more than 5 years, or fined not more than $250,000, or both.

44 USC 3501 note.

44 USC 3501 note.

PUBLIC LAW 107–347—DEC. 17 2002 116 STAT. 2967

Subtitle B—Statistical Efficiency

SEC. 521. FINDINGS AND PURPOSES.

(a) FINDINGS.—The Congress finds the following:

(1) Federal statistics are an important source of information for public and private decision-makers such as policymakers, consumers, businesses, investors, and workers.

(2) Federal statistical agencies should continuously seek to improve their efficiency. Statutory constraints limit the ability of these agencies to share data and thus to achieve higher efficiency for Federal statistical programs.

(3) The quality of Federal statistics depends on the willingness of businesses to respond to statistical surveys. Reducing reporting burdens will increase response rates, and therefore lead to more accurate characterizations of the economy.

(4) Enhanced sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics for exclusively statistical purposes will improve their ability to track more accurately the large and rapidly changing nature of United States business. In

particular, the statistical agencies will be able to better ensure that businesses are consistently classified in appropriate industries, resolve data anomalies, produce statistical samples that are consistently adjusted for the entry and exit of new businesses in a timely manner, and correct faulty reporting errors quickly and efficiently.

(5) The Congress enacted the International Investment and Trade in Services Act of 1990 that allowed the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics to share data on foreign-owned companies. The Act not only expanded detailed industry coverage from 135 industries to over 800 industries with no increase in the data collected from respondents but also demonstrated how data sharing can result in the creation of valuable data products.

(6) With subtitle A of this title, the sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics continues to ensure the highest level of confidentiality for respondents to statistical surveys.

(b) PURPOSES.—The purposes of this subtitle are the following:

(1) To authorize the sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics for exclusively statistical purposes.

(2) To reduce the paperwork burdens imposed on businesses that provide requested information to the Federal Government.

(3) To improve the comparability and accuracy of Federal economic statistics by allowing the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics to update sample frames, develop consistent classifications of establishments and companies into industries, improve coverage,

and reconcile significant differences in data produced
by the three agencies.
(4) To increase understanding of the United States
economy, especially for key industry and regional statistics,
44 USC 3501
note.

to develop more accurate measures of the impact of technology
on productivity growth, and to enhance the reliability of the
Nation's most important economic indicators, such as the
National Income and Product Accounts.

SEC. 522. DESIGNATION OF STATISTICAL AGENCIES.

For purposes of this subtitle, the term ''Designated Statistical
Agency'' means each of the following:
(1) The Bureau of the Census of the Department of Commerce.
(2) The Bureau of Economic Analysis of the Department
of Commerce.
(3) The Bureau of Labor Statistics of the Department of
Labor.

SEC. 523. RESPONSIBILITIES OF DESIGNATED STATISTICAL AGENCIES.

The head of each of the Designated Statistical Agencies shall—
(1) identify opportunities to eliminate duplication and
otherwise reduce reporting burden and cost imposed on the
public in providing information for statistical purposes;
(2) enter into joint statistical projects to improve the quality
and reduce the cost of statistical programs; and
(3) protect the confidentiality of individually identifiable
information acquired for statistical purposes by adhering to

safeguard principles, including—

(A) emphasizing to their officers, employees, and agents the importance of protecting the confidentiality of information in cases where the identity of individual respondents can reasonably be inferred by either direct or indirect means;

(B) training their officers, employees, and agents in their legal obligations to protect the confidentiality of individually identifiable information and in the procedures that must be followed to provide access to such information;

(C) implementing appropriate measures to assure the physical and electronic security of confidential data;

(D) establishing a system of records that identifies individuals accessing confidential data and the project for which the data were required; and

(E) being prepared to document their compliance with safeguard principles to other agencies authorized by law to monitor such compliance.

SEC. 524. SHARING OF BUSINESS DATA AMONG DESIGNATED STATISTICAL AGENCIES.

(a) IN GENERAL.—A Designated Statistical Agency may provide business data in an identifiable form to another Designated Statistical Agency under the terms of a written agreement among the agencies sharing the business data that specifies—

(1) the business data to be shared;

(2) the statistical purposes for which the business data are to be used;

(3) the officers, employees, and agents authorized to examine the business data to be shared; and

(4) appropriate security procedures to safeguard the confidentiality

of the business data.

(b) RESPONSIBILITIES OF AGENCIES UNDER OTHER LAWS.—The provision of business data by an agency to a Designated Statistical

44 USC 3501 note.

44 USC 3501 note.

44 USC 3501 note.

Agency under this subtitle shall in no way alter the responsibility of the agency providing the data under other statutes (including section 552 of title 5, United States Code (popularly known as the Freedom of Information Act), and section 552b of title 5, United States Code (popularly known as the Privacy Act of 1974)) with respect to the provision or withholding of such information by the agency providing the data.

(c) RESPONSIBILITIES OF OFFICERS, EMPLOYEES, AND AGENTS.—Examination of business data in identifiable form shall be limited to the officers, employees, and agents authorized to examine the individual reports in accordance with written agreements pursuant to this section. Officers, employees, and agents of a Designated Statistical Agency who receive data pursuant to this subtitle shall be subject to all provisions of law, including penalties, that relate—

(1) to the unlawful provision of the business data that would apply to the officers, employees, and agents of the agency that originally obtained the information; and

(2) to the unlawful disclosure of the business data that

would apply to officers, employees, and agents of the agency that originally obtained the information.

(d) NOTICE.—Whenever a written agreement concerns data that respondents were required by law to report and the respondents were not informed that the data could be shared among the Designated Statistical Agencies, for exclusively statistical purposes, the terms of such agreement shall be described in a public notice issued by the agency that intends to provide the data. Such notice shall allow a minimum of 60 days for public comment.

SEC. 525. LIMITATIONS ON USE OF BUSINESS DATA PROVIDED BY DESIGNATED STATISTICAL AGENCIES.

(a) USE, GENERALLY.—Business data provided by a Designated Statistical Agency pursuant to this subtitle shall be used exclusively for statistical purposes.

(b) PUBLICATION.—Publication of business data acquired by a Designated Statistical Agency shall occur in a manner whereby the data furnished by any particular respondent are not in identifiable form.

SEC. 526. CONFORMING AMENDMENTS.

(a) DEPARTMENT OF COMMERCE.—Section 1 of the Act of January 27, 1938 (15 U.S.C. 176a) is amended by striking ''The'' and inserting ''Except as provided in the Confidential Information Protection and Statistical Efficiency Act of 2002, the''.

(b) TITLE 13.—Chapter 10 of title 13, United States Code, is amended—

(1) by adding after section 401 the following:

''§ 402. Providing business data to Designated Statistical Agencies

''The Bureau of the Census may provide business data to the Bureau of Economic Analysis and the Bureau of Labor Statistics

(‘Designated Statistical Agencies’) if such information is required for an authorized statistical purpose and the provision is the subject of a written agreement with that Designated Statistical Agency, or their successors, as defined in the Confidential Information Protection and Statistical Efficiency Act of 2002.’’; and

44 USC 3501 note.

44 USC 3501 note.

Public information.

116 STAT. 2970 PUBLIC LAW 107–347—DEC. 17 2002

LEGISLATIVE HISTORY—H.R. 2458 (S. 803):

HOUSE REPORTS: No. 107–787, Pt. 1 (Comm. on Government Reform).

SENATE REPORTS: No. 107–174 accompanying S. 803 (Comm. on Governmental Affairs).

CONGRESSIONAL RECORD, Vol. 148 (2002):

Nov. 14, considered and passed House.

Nov. 15, considered and passed Senate.

WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 38 (2002):

Dec. 17, Presidential statement.

附錄二 澳洲電子化政府法

The Austrian E-Government Act

Federal Act on Provisions Facilitating Electronic Communications with Public Bodies

(Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen,

E-Government-Gesetz - E-GovG)

Published in the Austrian Federal Law Gazette (BGBl), part I, Nr. 10/2004, entered into force on 1 March 2004;

amended by BGBl I Nr. 7/2008 (amendments entered into force on 1 January 2008)

including the Corrigendum in BGBl I Nr. 59/2008

Table of Contents

Part I

Objects and Aims of the Act

1.

Part II

Identification and Authentication in Electronic Communications with Public Bodies

2. Definitions
3. Identity and Authenticity
4. The "Citizen Card" Function
5. Citizen Card and Representation
6. Source Identification Number (sourcePIN)
7. SourcePIN Register Authority
8. Unique Identification in Data files
9. ssPINs
10. Generation of ssPINs
11. Disclosure of ssPINs in Communications
12. Protection of the sourcePIN of Natural Persons

13. Further Guarantees for the Protection of ssPINs

Part III

Use of the Citizen Card Functions in the Private Sector

14. Generation of ssPINs for use in the private sector

15. Guarantees for the Protection of sourcePIN and ssPIN when used in the private sector

Part IV

Electronic Validation of Data

16. Information on Economic Activity as a Self-Employed Person

17. Data concerning Personal Status and Nationality

18. Other Data

Part V

Peculiarities of the Electronic Maintenance of Records

19. Official Signature

20. Probative Value of Printouts

21. Submission of Electronic Records

Part VI

Penal Provisions

22. Prohibited Use of sourcePIN, ssPIN or Official Signatures

Part VII

Transitional and Final Provisions

23. Linguistic Equal Treatment

24. Entry into Force

25. Transitional Provisions

26. Adoption and Entry into Force of Regulations

27. References

28. Implementation

Part I

Object and Aims of the Act

1 (1) The object of this Federal Act is to promote legally relevant electronic

communication. Electronic
communications with public bodies are to be facilitated, having regard to the principle of freedom to choose
between different means of communication when making submissions to such bodies.
(2) In order to improve legal protection, specific technical means shall be created to counter the risks associated
with an increased use of automated data processing for the purposes of achieving the aims set out in
subparagraph 1 and implemented where other precautions do not already provide adequate protection.
(3) With respect to implementation of the aims of this Federal Act, measures shall be taken to ensure that official
Internet sites which provide information or electronic support for procedures are structured in such a way as to
comply with international standards for access to the worldwide web, including unhindered access for disabled
persons.

Part II

Identification and Authentication in Electronic Communications with Public Bodies

Definitions

2. For the purposes of this part of the Act, the following definitions shall apply:
1. "Identity": designation of a specific person (data subject, No 7) by means of data which are particularly
suitable to distinguish persons from each other, such as, in particular, name, date of birth and place of birth
but also, for example, company name or (alpha)numerical designations;
2. "Unique identity": designation of a specific person (data subject, No 7) by means of one or more features
enabling that data subject to be unmistakably distinguished from all other data

subjects;
3. (Deleted by BGBl. I No. 7/2008)
4. "Identification": the process necessary to validate or recognise identity;
5. "Authenticity": the genuine nature of a declaration of intent or act in the sense that the purported author of
that statement or act is in fact the actual author;
6. "Authentication": the process necessary to validate or recognise authenticity;
7. "Data subject": any natural or legal person or other association or institution having its own identity for the
purposes of legal or economic relations;
8. "Source identification number (sourcePIN)": a number which is attributable to a data subject to be
unambiguously identified and which also serves as the basis for generating sector-specific personal
identifiers (ssPINs) (Paragraphs 9 and 14);
9. "Register of sourcePINs": a register used for the purpose of uniquely identifying data subjects and
comprising the technical components used, where necessary, for the generation of source identification
numbers;
10. "Citizen card": a logical unit that, independent of its technical implementation combines a qualified
electronic signature (Paragraph 2 3a SigG, BGBl. I No. 190/1999) with an identity link (Paragraph 4(2)) and
the associated security data and functions as well as any existing data on representation.

Identity and Authenticity

3. (1) In the context of electronic communications with controllers in the public sector within the meaning of
Paragraph 5(2) of the Datenschutzgesetz 2000 (Data Protection Act 2000), BGBl.

I 1 No 165/1999, rights of
access to personal data (Paragraph 4 No 1 of the Datenschutzgesetz 2000) in which there is a protected interest in
confidentiality within the meaning of Paragraph 1(1) of the Datenschutzgesetz 2000 may be granted only where
the unique identity of the person desiring access and the authenticity of his request have been validated. Such
validation must be provided in a form which can be verified electronically.
(2) Identification of a person may otherwise be requested in communications with controllers in the public sector
only insofar as this is necessary in an overriding legitimate interest of the controller, in particular, where it is an
essential requirement for performance of a task assigned to the controller by statute.

The "Citizen Card" Function

4. (1) The citizen card serves to validate the unique identity of a person making a submission and of the
authenticity of a submission made electronically in procedures for which a controller in the public sector has set
up a technical environment in which the citizen card can be used.
(2) The unique identification of a natural person who is the lawful holder of a citizen card shall be effected in
that person's citizen card by way of an identity link: the sourcePIN Register Authority (Paragraph 7) shall
confirm, by electronic signature, that the natural person identified in the citizen card as the holder has been
allocated a particular source identification number (sourcePIN) for the purpose of unique identification. With
respect to validation of identity in the event of representation, Paragraph 5 shall apply.

(3) The identity link shall be entered in the citizen card by the sourcePIN Register Authority or, on its behalf, by
other authorities or other appropriate bodies to be defined in more detail in the regulation to be adopted pursuant
to subparagraph 5. Whether a body is appropriate shall be assessed on the basis of whether it has the requisite
technology and the expertise necessary to be able to use it and of whether it can be relied upon to comply with
the legal framework conditions.
(4) The authenticity of a submission made using the citizen card shall be validated by the electronic signature
contained in the citizen card.
(5) Where necessary, detailed rules on subparagraphs 1 to 4 shall be laid down in a regulation of the Federal
Chancellor adopted with the consent of any other competent Federal Ministers. The Länder (Federal provinces)
and the local authorities, the latter represented by the local authorities' association and the municipal authorities'
association (Gemeindebund and Städtebund), shall be consulted prior to adoption of that regulation.

Citizen Card and Representation

5. (1) Where the citizen card is to be used for submissions by a representative, a reference to the permissibility of
the representation must be entered in the Citizen Card of the representative. This occurs where the sourcePIN
Register Authority, having been presented with proof of an existing authority to represent or in cases of statutory
representation, enters in the citizen card of the representative, upon application by the representative, the
sourcePIN of the data subject and a reference to the existence of an authority to

represent, including any relevant
material or temporal limitations. The permission to receive documents (Paragraph 35(3) second sentence of the
Service of Documents Act - ZustG;, BGBl. Nr. 200/1982) must be entered separately. Paragraph 4(3) shall apply
mutatis mutandis to the entries in the Citizen Card which are required .
(2) In cases of professional representation no particular proof of authority as in (1) to represent is required if the
general authority to represent is evident from the notice of professional entitlement according to the professional
regulations in the signature certificate. In this case, the sourcePIN Register Authority shall, upon application of
the professional representative, provide the sourcePIN of the data subject directly to the citizen card enabled
application where the official procedure is carried out. The general authority does not include the permission
according to Paragraph 35(3) second sentence ZustG.
(3) Provided that such a service is offered by authorities, officials (Organwalter) authorised especially for this
purpose may, at a person's request, lodge applications for that person with all authorities, irrespective of their
material and organisational competence, in procedures in which a Citizen Card may be used. The specific
instruction issued by the citizen shall be documented and kept by the authority in an appropriate form.
Applications shall be lodged using the citizen card of the official. The general competence of an official to lodge
applications for citizens must be apparent from the signature certificate in the official´s Citizen Card. In this
case, the sourcePIN Register Authority shall, upon application of the official,

provide the sourcePIN of the data
subject directly to the citizen card enabled application where the official procedure is carried out. The general
authority does not include the permission according to Paragraph 35(3) second sentence ZustG and the
authorisation for deliveries (Paragraph 9(1) ZustG).
(4) If the citizen card is used for acting as representative ((1)-(3)) it must be assured that
1. the sourcePIN of the representative is also provided to the citizen card enabled application
2. the sourcePINs are only used for the generation of ssPINs by the citizen card enabled application

Source Identification Number

6. (1) The person concerned shall be uniquely identified in the citizen card by his source identification number
(sourcePIN).
(2) With respect to natural persons who are registered in the Central Register of Residents (CRR), the source
identification number shall be derived from that person's registration number in the Central Register of Residents
(CRR number) (Paragraph 16(1) of the Meldegesetz 1991 (Registration Act 1991), BGBl. No 9/1992) and
secured by using strong cryptography. The source identification number of natural persons, not having to register
in the CRR, shall be derived on the basis of their registration number in a Supplementary Register (subparagraph
4). The use of the CRR number in order to generate the source identification number is not to be considered as a
use of data contained in the Central Register of Residents for the purposes of Paragraph 16a of the Meldegesetz

1991.
(3) For data subjects entered in the Register of Company Names, the Central Register of Associations or the
Supplementary Register the sourcePIN shall be the Register of Company Names number (Paragraph 3 (1) of the
Firmenbuchgesetz (Register of Company Names Act), BGBl. No 10/1991) or the Central Register of
Associations number (ZVR number) (Paragraph 18(3) of the Vereinsgesetz 2002 (Associations Act 2002),
BGBl. No 66/2002) or the registration number allocated in the Supplementary Register (subparagraph 4).
(4) Data subjects who are not entered in the Register of Residents and need not be entered in the Register of
Company Names nor in the Register of Associations shall be entered in the Supplementary Register upon
application or, in the cases of Paragraph 10(2) upon application of the client for the use of data by the SourcePIN
Register Authority (Paragraph 7) for proof of their unique identity. The condition in the case of natural persons is
the proof of the data laid down in the regulation of the Federal Chancellor to be adopted pursuant to Paragraph 4
(5) and in the case of other data subjects the proof of their legal existence including their legally valid name. The
process of issuing a citizen card requires proof of the identity data pursuant to Paragraph 1 (5a) MeldeG with
exception of the CRR number. The Supplementary Register shall be divided into sections for natural persons and
for other data subjects. The issue of authorities to act on behalf of others may also be entered in the section of the
Supplementary Register concerning data subjects who are not natural persons.

The domestic or foreign bodies to
which proof of the data required for registration in the Supplementary Register may be submitted and the bodies
authorised to enter the identity link in the citizen card shall be specified in the regulation of the Federal
Chancellor to be adopted pursuant to Paragraph 4(5). Moreover, that regulation shall govern the extent to which
the costs caused by contacting the sourcePIN Register Authority and the bodies instructed by it to verify identity
in connection with registration in the Supplementary Register and to enter references to representation must be
reimbursed; public bodies (Gebietskörperschaften) shall in any event be excluded from the duty to reimburse
such costs.
(5) Data subjects who are not registered in the Central Register of Residents nor in the Supplementary Register
may be entered in the Supplementary Register in the course of an application for the issue of a Citizen Card
without proof of the data in accordance with paragraph 4 if the application is provided with a qualified electronic
signature which is linked to an equivalent electronic verification of that person’s unique identity in his or her
country of origin. The Federal Chancellor shall lay down by Order further conditions for equivalence. The
sourcePIN Authority shall, upon application of the data subject, provide the SourcePIN of the data subject
directly to the citizen card enabled application where the official procedure is carried out. The sourcePIN may be
used by the SourcePIN Register Authority only to calculate ssPINs."
(6) For the generation of source identification numbers for natural persons the

sourcePIN Register Authority has
to use mathematical algorithms which apply strong cryptography to the sourcePIN. These algorithms shall be
determined by the sourcePIN Register Authority and - with the exception of the cryptographic key used -
published on the Internet.

sourcePIN Register Authority

7. (1) The sourcePIN Register Authority is the Data Protection Commission, which shall perform that function
by way of the Register for Data Files.
(2) In maintaining the Supplementary Register, generating source identification numbers and conducting the
procedures governed by Paragraphs 4, 9 and 10, the sourcePIN Register Authority may have recourse to the
Federal Ministry of the Interior as a service provider, insofar as natural persons are concerned, and to the Federal
Ministry of Finance, insofar as all other data subjects are concerned. The detailed provisions governing the
distribution of functions between the Data Protection Commission in its capacity as sourcePIN Register
Authority and the Federal Ministry of the Interior or the Federal Ministry of Finance as service providers shall be
laid down in a regulation of the Federal Chancellor after consultation of the Data Protection Commission and
with the consent of, as appropriate, the Federal Minister of the Interior or the Federal Minister for Finance. The
sourcePIN Authority shall randomly check that the tasks of the service providers are completed correctly..

Unique Identification in Data Files

8. In data files of controllers in the public sector, the identification of natural

persons within the framework of
the citizen card scheme may be represented only in the form of a ssPIN (Paragraph 9). With respect to persons
who are not natural persons, the source identification number may be stored for the purpose of unique
identification.

ssPINs

9. (1) The ssPIN is derived from the source identification number of the natural person concerned. The use of
that derived identifier for identification purposes shall be limited to that sector of State activity which is served
by the data file in which the ssPIN is to be used. The specific sector of State activity to which a data file is to be
allocated shall - to the extent that it is not governed by Paragraph 17(2) Nos 1 to 3 or (3) - be made apparent in
its registration in the Register of Data Files resp. in the Standard- und Muster-Verordnung (Regulation on
Standard and Model Data Processing) provided for in Paragraph 17(2) No 6 of the Datenschutzgesetz 2000.
(2) For the purpose of generating ssPINs, sectors of State activity are to be delimited in such a way as to ensure
that associated situations fall within the same sector and to prevent incompatible uses of data (Paragraph 6(1) No
2 of the Datenschutzgesetz 2000) within the same area. The description and delimitation of those areas shall be
determined in a regulation of the Federal Chancellor. The Länder and the local authorities, the latter represented
by the local authorities' association and the municipal authorities' association, shall be consulted prior to
adoption of that regulation.

(3) The mathematical algorithms applied to generate the ssPIN (hash function using the source identification
number und the sector code) shall be determined by the sourcePIN Register Authority and - with the exception
of any cryptographic keys used - published on the Internet.

Generation of ssPINs

10. (1) By the use of the citizen card a person's ssPIN is generated in electronic procedures for which a controller
in the public sector has created an environment in which the citizen card may be used. In sectors in which the
controller is not competent only encrypted (Paragraph 13(2)) ssPINs must be stored.
(2) The generation of SsPINs without the use of a citizen card is only allowed for the sourcePIN Register
Authority and is only permissible when unique identification on the basis of the ssPIN in data files of controllers
in the public sector is necessary because personal data are to be processed or transmitted in conformity with the
Datenschutzgesetz 2000. Such cases include, in particular, administrative cooperation, data acquisition at the
request of the data subject or a submission to an authority by a representative pursuant to Paragraph 5. In the
event of a request of ssPINs for a sector in which the controller is not competent to act as authority only ssPINs
which have been encrypted in accordance with Paragraph 13(2) may be made available.
(3) The reimbursement of the costs of the supply of ssPINs in connection with professional representation
pursuant to subparagraph 2 shall also be governed by the regulation to be adopted pursuant to Paragraph 4(5).

Disclosure of ssPINs in Communications

11. ssPINs shall not be stated in communications to data subjects or to third parties. The matching of such
communications to records of the controller concerning the same subject-matter shall be facilitated by other
means, such as a reference number.

Protection of the source Identification Number of Natural Persons

12. (1) Insofar as source identification numbers do not contain public data, such as the number of an entry in the
Register of Company Names or the ZVR number, their confidentiality shall be subject to special protection by
way of the following measures of the citizen card scheme:

1. The number derived from the CRR number and used as the source identification number of natural persons
may be permanently stored only in the citizen card and only in connection with the identity link or in order
to indicate an instance of authority to represent.

2. Source identification numbers of natural persons shall be generated in the sourcePIN Register whenever
they are required. They shall not, however, be subject to storage exceeding the time necessary for generation
and immediate transaction.

3. The use of the source identification number of natural persons in order to generate the ssPIN may not give
rise to any storage of the source identification number outside of the generation process.

4. Generating an ssPIN for use in the private sector (Paragraph 14) the computation from the source
identification number may not be carried out by the controller in the private sector.

(2) The source identification number may be used to generate a ssPIN only:
1. with the cooperation of the data subject by use of his citizen card; in each case, the data subject must be
informed accordingly of the electronic activation of the citizen card functions, or,
2. without the cooperation of the data subject, by the sourcePIN Register Authority in accordance with the
detailed provisions of Paragraphs 10 and 13(2).

Further Guarantees for the Protection of ssPINs

13. (1) ssPINs shall be generated by irreversible derivations from the source identification number. In the
interests of the transparency of State activity, this shall not apply to ssPINs which are used exclusively in
connection with the activity of a person as an official representing a public authority.
(2) Where it is permissible under Paragraph 10(2) to request from the sourcePIN Register Authority a ssPIN for
the purpose of the unique identification of a data subject, the sourcePIN Register Authority may, insofar as an
ssPIN for a sector in which the requester has no competence to act as authority is concerned, provide the ssPIN
in encrypted form only. The form of that encryption must be such as to ensure that:
1. only the controller in whose data file it is permissible to use the ssPIN in decrypted form is able to decrypt it
(subparagraph 3); and
2. as a result of the inclusion in the basis for encryption of additional variable data of which the requesting
party has no knowledge, the ssPIN cannot, even in encrypted form, supply any information on the data
subject.

(3) ssPINs may be stored in a data file in unencrypted form only where, in order to generate the ssPIN, use was
made of the code for the sector to which the data file is to be allocated in accordance with the regulation to be
adopted pursuant to Paragraph 9(2).

Part III

Use of the Citizen Card Functions in the Private Sector

Generation of ssPINs for use in the private sector

14. (1) For the identification of natural persons in electronic communications with a controller within the private
sector (Paragraph 5(3) of the Datenschutzgesetz 2000), an ssPIN may be derived using the citizen card, wherein
the sourcePIN of the controller replaces the sector code. This shall be subject to the condition that the controller
in the private sector has set up a technical environment in which the citizen card can be used and in which the
controller´s sourcePIN is made available as the sector code for generation of the ssPIN.
(2) Controllers in the private sector may store and use only such ssPINs that have been generated using their own
source identification number as sector code.

Guarantees for the Protection of Source Identification Numbers and ssPINs when used in the private

sector

15. (1) The generation of an ssPIN for use in the private sector requires the cooperation of the data subject with
the aid of the Citizen Card wherein the data subject must be instructed about the initiation of this function. It is
permissible without collaboration of the data subject and without using the citizen card if an unique

identification by means of ssPIN in applications of controllers of the private sector is necessary because

1. The controller has to establish the unique identity of his customers because of statutory provisions and

2. Personal data will be processed and transmitted in ways relevant to DSG 2000.

In such a case the generation of ssPINs may only be carried out by the ssPIN Register Authority.

(2) The sourcePIN of the data subject may not be made available to a controller in the private sector by way of

the citizen card functions at any time during the generation of the ssPIN.

Electronic verification of the accuracy

of the identity link used by the data subject is however possible by submitting a request for access to the Central

Residents Registry under Paragraph 16(1) of the Meldegesetz 1991.

Part IV

Electronic Validation of Data

Information on Economic Activity as a Self-Employed Person

16. (1) Electronic validation of the nature of a self-employed activity and of fulfilment of the professional

requirements for pursuit of that activity may be obtained from the Documentation Registry under Paragraph

114(2) of the Bundesabgabenordnung (Federal Fiscal Code).

(2) Where validation of the data referred to in subparagraph 1 is required in procedures involving a controller in

the public sector, the data subject may himself supply it by submitting a copy signed electronically by the

Documentation Registry or, at the request of the data subject, the controller may acquire it by way of electronic

access to the Documentation Register. It shall be permissible to obtain validation through official channels where

the statutory requirements for such data acquisition are satisfied.

Data concerning Personal Status and Nationality

17. (1) Where the accuracy of the data stored in the Central Register of Residents with regard to personal status
and nationality has been verified by the local registration authorities by way of inspection of the appropriate
documents (standard documents), those authorities must inform the Central Residents Registry thereof and the
fact that the data has been verified shall be noted in the Central Register of Residents in a suitable, electronically
legible form.
The data subject may request that such information be entered even outside a procedure for registration of
residence if he provides the registration authority with proof of the accuracy of the registration data by
submitting the appropriate documents.
(2) Where other authorities must determine, as a preliminary question in a procedure, the accuracy of data
relating to personal status or nationality which are also registration data, they may, provided that the person
concerned has consented to acquisition of the data or that such acquisition through official channels is authorised
by statute, submit an electronic request to the Central Residents Registry in that regard, which is to be treated in
accordance with Paragraph 16a(4) of the Meldegesetz 1991.
(3) The data subject may make use of the electronic availability of verified registration data by:
1. consenting to the acquisition of the data required from the Central Residents Registry in procedures in which
it is necessary to submit standard documents within the meaning of subparagraph

1; or
2. requesting from the Central Residents Registry a confirmation of registration which has been signed
electronically with an official signature (Paragraph 19) and which states that the accuracy of the individual
registration data has been verified.

Other Data

18. Authorities or persons on whom public powers have been conferred shall make public on the Internet the
extent to which they are prepared to issue electronic validation of the data stored by them within their area of
competence or operations. Validation which refers to personal data may be issued only to the person concerned
himself, or to third parties with the consent of the data subject only, unless acquisition of the data through
official channels is authorised by statute.

Part V

Peculiarities of Keeping Electronic Records

Official Signature

19. (1) An official signature, being the electronic signature of a public authority, is an advanced electronic
signature within the meaning of the Signaturgesetz (Signature Act), the peculiarity of which is indicated by an
appropriate attribute in the signature certificate.
(2) An official signature serves to facilitate recognition of the fact that a document originates from a controller in
the public sector. It may therefore only be used by this controller in accordance with the detailed conditions laid
down in subparagraph 3, when signing electronically or drawing up the documents issued by them.

(3) The official signature in views of electronic documents shall be displayed by means of an image which the
public sector controller has published on the Internet in secure form as its own and a reference within the
document confirming that it has been officially signed. The information needed for the validation of the
electronic signature has to be provided by the controller of the public sector.

Probative Value of Printouts

20. An electronic document of an authority printed out on to paper is assumed to be authentic (Paragraph 292
ZPO, RGBl. No. 113/1895) if signed with an official signature. The official signature has to allow verification by
reconverting the printout of the document into its electronic form or the document must be verifiable by other
means provided by the authority. The document shall include a reference to the source on the Internet,containing
the procedure for reconverting the printout into the electronic form and the applicable verification mechanisms,
or a reference to another verification process.

Submission of Electronic Records

21. (1) Where an authority is required to submit records to another authority and those records were generated
and approved electronically, the duty to submit relates to the electronic original. This applies, in particular, to
records which are kept in an entirely electronically operated file processing and management system. The
document must be submitted in a standard format.
(2) Standard formats are such electronic formats which, using the latest available technology, guarantee the best
legibility of a document possible, from the point of view of third parties also,

during the period for which it is
envisaged that the document is to be kept.
(3) Where the authority to which the electronic record is to be submitted has authorised an electronic delivery
service to receive correspondence addressed to it, the record may also be submitted to that agent, in particular,
where proof of submission is required.
In such cases, the provisions in Part III of the Zustellgesetz (Service of Documents Act) shall apply mutatis
mutandis, subject to the condition that the document is to be considered as submitted on the day following the
electronic dispatch of notification that the document is available for retrieval from the server of the delivery
service.

Part VI

Penal Provisions

Prohibited Use of SourcePINs , ssPINS or Official Signatures

22. (1) Insofar as an act does not constitute a criminal offence which falls within the jurisdiction of the courts or
does not carry a more severe penalty in accordance with other provisions on administrative offences, an
administrative offence which may be penalised by the local administrative authority with a fine of up to EUR 20
000 is committed by any person who:
1. contrary to the provisions of Part II and III, obtains the source identification number or ssPIN of a natural
person with a view to using them in order to acquire unlawfully personal data of the data subject; or
2. stores or uses an ssPIN of another controller in the private sector without authorisation; or

3. makes available to other controllers in the private sector an ssPIN derived from his own source identification
number in a manner prohibited under Paragraph 8 of the Datenschutzgesetz 2000;
or
4. uses an ssPIN in order to supply third parties with data concerning a registered domicile of the data subject;
or
5. uses or purports to use an official signature contrary to Paragraph 19(2).
(2) The penalty of forfeit of objects (Paragraphs 10, 17 und 18 of the Verwaltungsstrafgesetz 1991
(Administrative Offences Act)) which have been acquired in connection with an administrative offence within
the meaning of subparagraph 1 may be imposed.
(3) The authority in whose district the offence was committed shall have territorial jurisdiction to give decisions
under subparagraphs 1 and 2.

Part VII

Transitional and Final Provisions

Linguistic Equal Treatment

23. Insofar as the terms in this Article referring to natural persons are worded only in the masculine form, they
shall apply to men and women equally.

Entry into Force

24. With the exception of Part IV, this Federal Act shall enter into force on 1 March 2004. Part IV shall enter
into force on 1 January 2005.
(2) The table of contents, Par. 1 (3), Par. 2 No. 8 and 10, Par. 3 (1), Par. 5, Par. 6 (2) to (6), Par. 7 (2), Par. 8, the
heading before Par. 9, Par. 9 (1) and (2), the heading before Par. 10, Par. 10 (1) to (3), the heading before

Par. 11, Par. 11, Par. 12 (1) No. 4 and (2), the heading before Par. 13, Par. 13 (1) to (3), the heading before
Par. 14, Par. 14 (1) and (2), the heading before Par. 15, Par. 15 (1) and (2), Par. 19 (1) to (3), Par. 20, the heading
before Par. 22, Par. 22 (1) No. 1 to 4 and Par. 25 (1) to (3) in the version of BGBl. I Nr. 7/2008 come into force
on 1 January 2008; at the same time Par. 2 No. 3 expires.

Transitional Provisions

25. (1) Until 31 December 2007, administrative signatures may also be used in connection with citizen card
functions and shall be treated in the same way as secure signatures.
Administrative signatures are signatures which, within the limits of the scope of their permissible use, provide
sufficient security even if they do not necessarily satisfy all the conditions for the generation and storage of data
used to create qualified signatures and are not necessarily based on a qualified certificate. The security and
organisational conditions which must be fulfilled by an administrative signature for the purposes of this Federal
Act shall be laid down in a regulation of the Federal Chancellor.
(2) In cases in which laws beneath the constitutional level expressly require the use of a qualified electronic
signature in communications with public bodies exercising official authority (Hoheitsverwaltung), that condition
shall be regarded as fulfilled even where an administrative signature is used, until expiry of the transitional
period referred to in subparagraph 1.
(3) Within the context of the Citizen Card function the administrative signatures issued on the basis of paragraph
1 shall be considered as equivalent to qualified signatures until the expiry of the

associated certificate, but no
later than 31.12.2012.

Adoption and Entry into Force of Regulations

26. Regulations based on this Federal Act, as it may be amended, may be adopted from the day following
proclamation of the statutory provisions to be implemented by them; however, they may not enter into force
before those statutory provisions.

References

27. Insofar as reference is made in this Federal Act to other Federal acts, those acts shall be applicable in the
version in force at the relevant time.

Implementation

28. The following organs shall be competent to implement this Federal Act:
1. with respect to Paragraph 4(5), the Federal Chancellor acting with the consent of any other competent
Federal Ministers,
2. with respect to Paragraph 7(2), the Federal Chancellor acting with the consent of the Federal Minister of the
Interior or the Federal Minister of Finance, depending on whether services relating to the source
identification numbers of natural persons or services relating to the source identification numbers of nonnatural
persons are concerned,
3. with respect to Paragraph 9(2), the Federal Chancellor,
4. with respect to the final sentence of Paragraph 15(2) and Paragraph 17, the Federal Minister if the Interior,
5. with respect to Paragraph 16, the Federal Minister of Finance,
6. as regards the remainder, any Federal Minister within his area of competence and to the extent that implementation is not a matter for the Federal Government

or the Governments of the Länder.

附錄三 馬來西亞電子化政府法

1

LAWS OF MALAYSIA

Act 680

ELECTRONIC GOVERNMENT ACTIVITIES ACT 2007

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

Section

1. Short title and commencement
2. Application
3. Use not mandatory
4. Reference to other written laws
5. Interpretation

PART II

ADMINISTRATION AND APPLICATION

OF THE ACT TO WRITTEN LAW

6. Designation by relevant Minister
7. Subsidiary legislation
8. Repeal or amendment
9. Information Technology Instructions

PART III

LEGAL RECOGNITION OF ELECTRONIC MESSAGE

10. Legal recognition of electronic message
11. Formation and validity of contract

PART IV

FULFILMENT OF LEGAL REQUIREMENTS BY ELECTRONIC MEANS

12. Writing
13. Signature
14. Seal
15. Witness
16. Original
17. Certified true copy
18. Copy
19. Submission of a document
20. Prescribed form
21. Requirement to issue licence, permit, approval, authorization, *etc.*
22. Retention of document
23. Electronic register
24. Service and delivery
25. Personal service
26. Payment
27. Receipt

PART V

COMMUNICATION OF ELECTRONIC MESSAGE

28. Attribution of electronic message
29. Contents of electronic message
3
30. Each electronic message to be regarded separately
31. Time of dispatch
32. Time of receipt
33. Place of dispatch
34. Place of receipt
35. Acknowledgement of receipt

PART VI

MISCELLANEOUS

36. Regulations

SCHEDULES

LAWS OF MALAYSIA

Act 680

ELECTRONIC GOVERNMENT ACTIVITIES ACT 2007

An Act to provide for legal recognition of electronic messages in dealings between the Government and the public, the use of the electronic messages to fulfill legal requirements and to enable and facilitate the dealings through the use of electronic means and other matters connected therewith.

ENACTED by the Parliament of Malaysia as follows:

PART I

PRELIMINARY

Short title and commencement

1. (1) This Act may be cited as the Electronic Government Activities Act 2007.

(2) This Act comes into operation on a date to be appointed by the Minister by notification in the *Gazette*.

Application

2. Subject to section 3, this Act shall apply to Federal laws which are designated in accordance with section 6.

5

Use not mandatory

3. (1) Nothing in this Act shall make it mandatory for a person to use, provide or accept any electronic message in dealings with the Government unless the person consents to the using, providing or accepting of the electronic message.

(2) A person's consent to use, provide or accept any electronic message in dealings with the Government may be inferred from the person's conduct.

Reference to other written laws

4. The application of this Act shall be supplemental and without prejudice to any other written laws regulating the dealings between the Government and the public.

Interpretation

5. In this Act, unless the context otherwise requires —

"designated Act" means a written law or part of it which is designated by the relevant Minister under section 6;

"Information Technology Instructions" means the instructions issued under section 9;

"electronic" means the technology of utilizing electrical, optical, magnetic, electromagnetic, biometric, photonic or other similar technology;

"Minister" means the Minister charged with the responsibility for leading the changes in modernizing the Malaysian public service administration;

6

"relevant Minister" means the Minister charged with the responsibility for the administration of the designated Act;

"electronic message" means an information generated, sent, received or stored by an electronic means;

"originator" means a person by whom or on whose behalf, the electronic message is generated or sent;

"addressee" means a person who is intended by the originator to receive the electronic message;

"information processing system" means an electronic system for generating, sending, receiving, storing or processing the electronic message;

"electronic signature" means any letter, character, number, sound or any other symbol or any combination thereof created in an electronic form adopted by a person as a signature.

PART II

ADMINISTRATION AND APPLICATION OF ACT TO WRITTEN LAW

Designation by relevant Minister

6. (1) The relevant Minister may, after consultation with the Minister, designate in Form 1 of the Schedule, any written law or part of it for the purpose of the application of this Act.

(2) The relevant Minister, in designating any written law or part of it under subsection (1), may impose any conditions as he deems fit.

7

Subsidiary legislation

7. (1) This Act shall be deemed to apply to any subsidiary legislation of a designated Act unless excluded in accordance with subsection (2).

(2) The relevant Minister may, by notification in Form 2 of the Schedule, after consultation with the Minister, exclude any subsidiary legislation of a designated Act from the application of this Act.

(3) The relevant Minister may, by notification in Form 3 of the Schedule, after consultation with the Minister, include any subsidiary legislation which has been excluded under subsection (2), for the purpose of the application of this Act.

Repeal or amendment

8. (1) Where a designated Act is repealed, such repealed Act shall no longer be the designated Act from the effective date of its repeal save for the subsidiary legislation unaffected by the repeal of the designated Act.

(2) Where a designated Act is amended and the relevant Minister is satisfied that the amended Act is inconsistent with the policy or objectives of this Act, the relevant Minister may, in Form 4 of the Schedule, exclude the amended Act or part thereof from the application of this Act.

Information Technology Instructions

9. (1) The Minister may issue Information Technology Instructions which may include –

(a) information technology standards*;*

8

(b) the criteria for the electronic signature and appropriate seal for the purpose for which they are used;

(c) the process of recording the time and acknowledgment of receipt of the electronic message;

(d) security measures against any unauthorized access;

(e) disaster recovery procedures;

(f) accessibility rules for electronic government services and forms;

(g) management and maintenance of the electronic message;

(h) methods relating to data entry and verification of the electronic message;

(i) guidelines for the payment and receipt of money; and

(j) any other matters as may be required from time to time.

(2) Non-compliance with any of the Information Technology Instructions shall not affect the validity or enforceability of the activities, which are undertaken electronically pursuant to this Act.

PART III

LEGAL RECOGNITION OF ELECTRONIC MESSAGE

Legal recognition of electronic message

10. (1) Any information shall not be denied legal effect, validity or enforceability on the ground that it is wholly or partly in an electronic form.

9

(2) Any information shall not be denied legal effect, validity or enforceability on the ground that the information is not contained in the electronic message that gives rise to such legal effect, but is merely referred to in that electronic message, provided that the information being referred to is accessible to the person against whom the referred information might be used.

Formation and validity of contract

11. (1) In the formation of a contract, the communication of proposals, acceptance of proposals, and revocations of proposals and acceptances or any

related communication may be expressed by an electronic message.
(2) A contract shall not be denied legal effect, validity or enforceability on the ground that an electronic message is used in its formation.

PART IV

FULFILMENT OF LEGAL REQUIREMENTS BY ELECTRONIC MEANS

Writing

12. Where any law requires information to be in writing, the requirement of the law is fulfilled if the information is contained in an electronic message that is accessible and intelligible so as to be usable for subsequent reference.

Signature

13. (1) Where any law requires a signature of a person on a document, the requirement of the law is fulfilled, if the document is in the form of an electronic message, by an electronic signature which –
(a) is attached to or is logically associated with the electronic message;
10
(b) adequately identifies the person and adequately indicates the person's approval of the information to which the signature relates; and
(c) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.
(2) For the purposes of paragraph (1)*(c)*, an electronic signature is as reliable as is appropriate if –
(a) the means of creating the electronic signature is linked to and under the control of that person only;
(b) any alteration made to the electronic signature after the time of signing is detectable; and
(c) any alteration made to that document after the time of signing is detectable.
(3) The Digital Signature Act 1997 [*Act 562*] shall continue to apply to

any digital signature used as an electronic signature in any Government activities.

Seal

14. (1) Where any law requires a seal to be affixed to a document, the requirement of the law is fulfilled, if the document is in the form of an electronic message, by a digital signature as provided under the Digital Signature Act 1997.

(2) Notwithstanding subsection (1), the Minister may, by order in the *Gazette*, prescribe any other electronic signature that fulfills the requirement of affixing a seal in an electronic message.

11

Witness

15. Where any law requires the signature of a witness on a document, the requirement of the law is fulfilled, if the document is in the form of an electronic message, by an electronic signature of the witness which complies with the requirement of section 13.

Original

16. (1) Where any law requires any document to be in its original form, the requirement of the law is fulfilled by a document in the form of an electronic message if –

(a) there exists a reliable assurance as to the integrity of the information contained in the electronic message from the time it is first generated in its final form; and

(b) the electronic message is accessible and intelligible so as to be usable for subsequent reference.

(2) For the purposes of subparagraph (1)*(a)* –

(a) the criteria for assessing the integrity of the information shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of

communication, storage and display; and
(b) the standard of reliability required shall be assessed in the light of the purpose for which the document was generated and in the light of all other relevant circumstances.
12

Certified true copy

17. Where any law requires submission of a certified true copy of a document, the requirement of the law is fulfilled if the document is submitted in the form of an electronic message and fulfills the requirement under section 16.

Copy

18. Where any law requires any document to be retained, served, sent or delivered in more than one copy, the requirement of the law is fulfilled, if the document is in the form of an electronic message, by retention, service, sending or delivery of the document in one copy.

Submission of a document

19. (1) Where any law requires the filing or submission of any document, the requirement of the law is fulfilled, if the document is filed or submitted in the form of an electronic message, if the electronic message is accessible and intelligible so as to be usable for subsequent reference.
(2) For the purposes of subsection (1), where any prescribed form is specified by an electronic means, the filing or submission of such document shall be in accordance with such specified form.

Prescribed form

20. Where any law requires any document to be in a prescribed form, the requirement of the law is fulfilled by a document in the form of an electronic message if the electronic message is –
13
(a) formatted in the same or substantially the same way as the prescribed form;
(b) accessible and intelligible so as to be usable for subsequent

reference; and

(c) capable of being retained by the other person.

Requirement to issue licence, permit, approval, authorization, *etc.*

21. Where any law requires the issuance of any licence, permit, approval, authorization or similar document, the requirement of the law is fulfilled if the licence, permit, approval, authorization or similar document is issued in the form of an electronic message provided that the electronic message is accessible and intelligible so as to be usable for subsequent reference.

Retention of document

22. Where any law requires any document to be retained, the requirement of the law is fulfilled by retaining the document in the form of an electronic message if the electronic message –

(a) is retained in the format in which it was generated, sent or received, or in a format that does not materially change the information contained in the electronic message that was originally generated, sent or received;

(b) is accessible and intelligible so as to be usable for subsequent reference; and

(c) identifies the origin and destination of the electronic message and the date and time it was sent or received.

14

Electronic register

23. (1) Where any law requires a register to be established, operated and maintained, the requirement of the law is fulfilled if the register is in the form of an electronic message and its contents cannot be altered by any means by any person administering the register who has the power by law to alter the register.

(2) Any search made on a register established, operated and maintained by an electronic message shall have the same legal validity as the register referred to in a designated Act.

Service and delivery

24. (1) Where any law requires any document to be served, sent or delivered, the requirement of the law is fulfilled by the service, sending or delivery of the document by an electronic means if an information processing system is in place –

(a) to identify the origin, destination, time and date of service, sending or delivery; and

(b) for the acknowledgement of receipt,

of the document.

(2) This section does not apply to –

(a) any notice of default, notice of demand, notice to show cause, notice of repossession or any similar notices which are required to be served prior to commencing a legal proceeding; and

15

(b) any originating process, pleading, affidavit or other documents which are required to be served pursuant to a legal proceeding.

Personal service

25. Where any law requires a document to be submitted or delivered personally, the requirement of the law is fulfilled if the document is submitted in accordance with section 19 accompanied with an electronic signature.

Payment

26. Where any law requires any payment to be made, the requirement of the law is fulfilled if the payment is made by an electronic means and complies with any conditions imposed by the Government.

Receipt

27. Where any law requires the issuance of any receipt of payment, the requirement of the law is fulfilled if the receipt is in the form of an electronic message and the electronic message is accessible and intelligible so as to be usable for subsequent reference.

PART V

COMMUNICATION OF ELECTRONIC MESSAGE

Attribution of electronic message

28. (1) An electronic message is that of the originator if it is sent by the originator himself.

(2) As between the originator and the addressee, an electronic message is deemed to be that of the originator if it is sent by –

16

(a) a person who has the authority to act on behalf of the originator in respect of that electronic message; or

(b) an information processing system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard an electronic message as being that of the originator, and to act on that presumption, if –

(a) the addressee properly applies an authentication method agreed between the originator and the addressee for ascertaining whether the electronic message was that of the originator; or

(b) the electronic message as received by the addressee resulted from the actions of a person whose relationship with the originator or any agent of the originator enabled that person to gain access to an authentication method used by the originator to identify electronic message as its own.

(4) Subsection (3) does not apply if –

(a) the addressee has received a notice from the originator that the electronic message is not that of the originator and has reasonable time to act accordingly; or

(b) the addressee knew or should have known that the

electronic message was not that of the originator had he exercised reasonable care or used any authentication method agreed between the originator and the addressee.

17

Contents of electronic message

29. Where an addressee receives an electronic message, the addressee is entitled to regard the electronic message as being what the originator intended to send, and to act on that presumption, unless the addressee knew or should have known, had he exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the electronic message as received.

Each electronic message to be regarded separately

30. Where an addressee receives an electronic message, the addressee is entitled to regard each electronic message received as a separate electronic message and to act on that presumption, unless the addressee knew or should have known, had he exercised reasonable care or used any agreed procedure, that the electronic message was a duplicate.

Time of dispatch

31. Unless otherwise agreed between the originator and the addressee, an electronic message is deemed sent when it enters an information processing system outside the control of the originator.

Time of receipt

32. Unless otherwise agreed between the originator and the addressee, an electronic message is deemed received –

(a) where the addressee has designated an information processing system for the purpose of receiving electronic messages, when the electronic message enters the designated information processing system; or

18

(b) where the addressee has not designated an information

processing system for the purpose of receiving electronic messages, when the electronic message comes to the knowledge of the addressee.

Place of dispatch

33. Unless otherwise agreed between the originator and the addressee, an electronic message is deemed sent from the originator's place of dealing, and –

(a) where the originator has more than one place of dealings, from the place of dealing that has the closest relationship with the dealing or where there is no place of dealing that has the closest relationship with the dealing, from the originator's principal place of dealing; or

(b) where the originator does not have a place of dealing, from the originator's ordinary place of residence.

Place of receipt

34. Unless otherwise agreed between the originator and the addressee, an electronic message is deemed received at the addressee's place of dealing, and –

(a) where the addressee has more than one place of dealings, at the place of dealing that has the closest relationship with the dealing or where there is no place of dealing that has the closest relationship with the dealing, at the addressee's principal place of dealing; or

(b) where the addressee does not have a place of dealing, at the addressee's ordinary place of residence.

19

Acknowledgement of receipt

35. (1) This section applies where, on or before sending an electronic message, or in the electronic message, the originator has requested or agreed with the addressee that receipt of the electronic message is to be acknowledged.

(2) Where the originator has requested or agreed with the addressee that receipt of the electronic message is to be acknowledged, the electronic message is treated as though it has never been sent until the acknowledgement is received.
(3) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by –
(a) any communication by the addressee, automated or otherwise; or
(b) any conduct of the addressee sufficient to indicate to the originator that the electronic message has been received.
(4) Where the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator may –
(a) give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and
(b) if the acknowledgement is not received within the time specified in paragraph *(a)*, give notice to the addressee to
20
treat the electronic message as though it had never been sent and exercise any other rights he may have.
(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the addressee received the related electronic message.
(6) Where the received acknowledgement states that the related electronic message fulfills technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been fulfilled.

PART VI

MISCELLANEOUS

Regulations

36. The Minister may make such regulations as may be necessary or expedient for giving full effect to the provisions of this Act.

SCHEDULE

FORM 1

[Section 6]

ELECTRONIC GOVERNMENT ACTIVITIES ACT 2006

NOTIFICATION OF DESIGNATED ACT

IN exercise of the powers conferred by section 6 of the Electronic Government Activities Act 2006 [*Act*], I ……,

[*name of the relevant Minister*]

Minister of ……..……, after consultation with the Minister, designate –

……
…

[*name of the Act or part of it*]

as a designated Act under the Electronic Government Activities Act 2006.

2. The Electronic Government Activities Act 2006 shall apply to the provisions of the Act and the subsidiary legislation made under the Act subject to the following:

……
…

……
…

……
…

3. This Notification comes into operation on…….. [*specify the date*].

Dated

[*Name of the relevant Minister*]

Minister of [*specify the Ministry*]

FORM 2

[Subsection 7(2)]

ELECTRONIC GOVERNMENT ACTIVITIES ACT 2006

NOTIFICATION OF EXCLUSION OF SUBSIDIARY LEGISLATION FROM THE ACT

IN exercise of the powers conferred by subsection 7(2) of the Electronic Government Activities Act 2006 [*Act*], I

……..……., Minister of

[*name of the relevant Minister*]

……..……, after consultation with the Minister, exclude –

……
…

[*name of the subsidiary legislation*]

made under

……
…

[*name of the designated Act*]

from the application of the Electronic Government Activities Act 2006.

2. This Notification comes into operation on……. [*specify the date*].

Dated

[*Name of the relevant Minister*]

Minister of [*specify the Ministry*]

FORM 3

[Subsection 7(3)]

ELECTRONIC GOVERNMENT ACTIVITIES ACT 2006

NOTIFICATION OF INCLUSION OF SUBSIDIARY LEGISLATION FOR THE APPLICATION OF THE ACT

IN exercise of the powers conferred by subsection 7(3) of the Electronic Government Activities Act 2006 [*Act*], I …….,

[*name of the relevant Minister*]
Minister of ……..., after consultation with the Minister, include –
……
…
[*name of the subsidiary legislation*]
made under
……
…
[*name of the designated Act*]
for the purpose of the application of the Electronic Government Activities Act 2006.
2. This Notification comes into operation on……. [*specify the date*].
Dated
[*Name of the relevant Minister*]
Minister of [*specify the Ministry*]

FORM 4

[Subsection 8(2)]

ELECTRONIC GOVERNMENT ACTIVITIES ACT 2006

NOTIFICATION OF EXCLUSION OF AMENDED ACT FROM THE ACT

IN exercise of the powers conferred by subsection 8(2) of the Electronic Government Activities Act 2006 [*Act*], I
……..……., Minister of
[*name of the relevant Minister*]
……..……, exclude –
(a) the whole of ……..….. (*name of the amended Act*); or
(b) part of ……..… (*name of the amended Act*), as follows:
(i) …….……;

(ii) ……..…..; and

(iii) ……..…., (*please specify*)

from the application of the Electronic Government Activities Act 2006.

2. This Notification comes into operation on

…… [*specify the date*].

Dated

[*Name of the relevant Minister*]

Minister of [*specify the Ministry*]

附錄四 菁英訪談名單

	任職機關	位階	身分	性別
A-01	資策會	高級幕僚	現任	男
A-02	台北市政府資訊中心	高級主管	現任	男
A-03	行政院研考會	高級主管	現任	男
A-04	行政院政務委員	高級幕僚/主管	卸任	男
A-05	行政院顧問	高級幕僚	卸任	女

附錄五 菁英訪談題綱

1. 有關電子化政府進程的「組織安排」與「規劃程序」

（1）就您主政時期的經驗，我國政府 e 化的推動體系（如組織安排、職掌與相互關係）爲何？

（2）就您主政時期的經驗，我國政府部門電子化政府的計畫/方案是如何擬定的？規劃程序（特別是願景/目標訂定）爲何？政府內部參與的情形（單位、中央地方…）？政府外部有那些背景的人參與？如何參與（規劃委員、顧問會議…）？過去民眾是否有參與規劃的機會？如果未來要這樣作，您的意見爲何？

2. 試就以下層面（如附件），就您主政時期的經驗，提出寶貴看法：

（1）特定計畫/方案的時空背景（特別是「國際潮流」）爲何？對本案推動造成什麼影響？

（2）若和前階段比較，特定計畫/方案在「資通科技」上有何突破？

（3）若和前階段比較，特定計畫/方案在「資訊安全」上克服哪些議題？

（4） 若和前階段比較，特定計畫/方案在「資訊法制」上有何進展？

（5） 若和前階段比較，特定計畫/方案在「行政運作」上有何提升？

（6） 若和前階段比較，特定計畫/方案在「社會互動」上有何精進？

（7） 整體上，特定計畫/方案的階段性貢獻？

（8） 是否仍有遺漏其他層面的表現，值得補充說明？

3. 政府部門成功推展一項 e 化創新服務甚爲可貴，就您觀察：

（1）從執行過程來看，e 化創新服務的擴散面臨哪些典型的阻力？（如實用性、信任、工作實務相容性等…）

（2）從時間序列角度來看，e 化創新服務的提供有何特徵？（如演化…）

附錄六 2020 台灣電子治理願景工作坊計畫書

2020 台灣電子治理
願景工作坊

計畫書

計畫主持人：政治大學公共行政學系 陳敦源副教授
協同主持人：世新大學行政管理學系 胡龍騰助理教授
淡江大學公共行政學系 曾冠球助理教授

中 華 民 國 九 十 七 年 八 月

壹、緣起

願景工作坊(Scenario Workshop)是一種具有審議民主精神的公民參與模式；透過願景工作坊的舉辦，參與者可對於所關懷的事務或議題，共同描繪未來發展的願景與藍圖。

在工作坊的實際運作過程中，參與者將根據他們的經驗與期盼，檢視這些願景。願景工作坊強調收集參與者對於討論議題的看法與認知，以及與會者對於未來發展的態度與他們關切的項目。經過批判、提出觀點與思考願景的過程，提出他們的看法以及具體可行的行動方案。

本次願景工作坊的討論主題爲台灣2020電子化治理未來願景的規劃，不同於以往的公民參與模式，台灣2020電子化治理願景工作坊將突破「由上而下」或「由下而上」的單線運作模式，而以類似於網絡參與的方式擴大參與基礎。規劃中參與會議的人員將包含中央與地方層級之政府官員、業界、非營利組織及一般民眾。期望透過此一願景工作坊之舉辦，能使不同利害關係人對於電子治理未來願景，能夠相互對話、相互理解，進而型塑彼此之共同願景。

貳、議題名稱

『2020台灣電子治理』願景工作坊。

參、工作團隊組成

團隊將由富有主持願景工作坊經驗之專家學者爲主，並將邀請經由行政院青輔會培力之具有審議民主主持人資格的青年二至三名，一同擔任主辦以及主持工作團隊成員。

肆、執行期間

97年9月27日(星期六)～9月28日(星期日)。

伍、會議地點

世新大學管理學院大樓（台北市文山區木柵路一段111號）。

陸、預定招募人數及招募方式

(一)政府官員8-10名：由本工作坊執行委員會遴選具有業務資歷或代表性之中央及地方政府資訊相關業務主管人員(或其代理人)。

業界代表8-10名：邀請曾參與我國政府電子化歷程的軟、硬體資訊廠商(如IBM)、網路及通訊媒體業界主管人員。

(二)**非營利組織代表8-10名**：邀請曾參與我國政府電子化歷程之非營利組織(如資策會)，以及關心我國資訊社會發展或數位落差現況之社會團體。

(三)公民代表8-10名：由願景工作坊負責小組以海報、文宣及網頁先做一普遍性的宣傳，結合「我的E政府」、全國社區大學、全國社區發展協會網站公布招募訊息，並透過政策網絡智庫會員進行與會公民的宣傳與招募，再由報名民眾中隨機抽樣，納入本次會議公民小組成員。

柒、會議進行方式

參考願景工作坊的模式進行，會議共進行兩日。本會議將提供參與者來往交通費用（大台北地區以外）、一天住宿、兩天保險與膳食（包含會議第一天午、晚餐與第二天早、午餐以及會議期間茶水、點心）。

捌、願景會議流程

正式會議第一天流程 (含提供住宿)。97 年 9 月 27 日星期六。

第一天議程	
時間	議程
09:00-09:30	報到
09:30-09:50	開幕式
09:50-10:50	專題演講一－台灣電子化治理相關政策與未來期許 發表人－宋餘俠 行政院研究發展考核委員會副主任委員
10:50-11:10	茶敘時間

11:10-12:10	專題演講二－願景工作坊介紹 發表人－林子倫 臺灣大學政治系助理教授
12:10-13:00	午餐時間
13:00-14:00	分組會議－我們的主張（初步願景）
14:00-15:30	分組會議－我們的願景
15:30-16:00	茶敘時間
16:00-16:40	全體會議－各組願景
16:40-18:00	全體會議－比較、釐清與回應
18:00	晚餐

正式會議第二天流程。97 年 9 月 28 日星期日。

第二天議程	
時間	議程
09:00-09:30	全體會議－會議進行方式說明與角色分組
09:30-12:00	分組會議－好點子初選
12:10-13:00	午餐時間
13:00-14:00	全體會議－好點子決選
14:00-15:00	全體會議－好點子亮相
15:00-15:30	茶敘時間
15:30-17:00	全體會議－好點子上路，未來會更好
17:00	賦歸

玖、預期成效

透過公共討論的過程，可以進一步將公民參與的意見加入政府的計畫之中，並透過實際深度的討論與對話，強化公民對台灣未來電子化治理願景規劃的想像。在此活動結束後，預期可達到以下效益：

(一)推廣並強化台灣民眾公民參與的精神，鼓勵公民能勇與表達自身意見，促進政府和民間的互動與合作。

(二)凝聚台灣全體公民對於電子化治理的共識，可使全體社會不同的利益和價值考量能達到一個均衡點，在此基礎下所進行的各項決策會更具正當性。

(三)透過公民參與的過程，一方面可以提升社會大眾應有之權益，另一方面更能讓民眾重視身爲台灣公民所應有的責任與義務。

(四)多元意見可以獲得融合，不光是政府單方面的主導政策，公民意見也能透過此次願景工作坊得以發聲，不同觀點的相互激盪和審慎思辯後的結論，才是真正足以作爲台灣2020年電子化治理的指導方針。

(五)使中央、地方和公民的願景能夠相容，並創造出屬於台灣自己的電子化治理指標,讓台灣能站上國際舞台與世界接軌並增加我國的國際競爭力。

拾壹、結語

21世紀電子化時代的降臨，對全球造成巨大的影響，對於政府的運作也同樣有著不可小覷的衝擊，各種嶄新的管理技術和觀念不斷出現，電子化政府儼然已成爲未來各國政府發展的主要方向。另一個近年來成爲主要討論議題的就是公民參與，過去的台灣公民在特殊的政治情勢下一直未能有實際的機會去參與政府政策的制定過程，然而公民參與的精神已是全球化時代下一股勢不可擋的風潮，我們必須去加以重視並確實地貫徹此一精神。

此次針對台灣2020電子化治理議題所進行的願景工作坊，創造出一個能給中央、地方政府和公民能夠溝通，凝聚集體共識的空間。經過此次願景工作坊能廣納各方對於台灣未來電子化治理的想法，相互交流經驗與知識，最終提出共同願景，這一方面強化了台灣未來政府電子化的進行，也能顧及到公民參與精神的實踐，使台灣能邁向更好的未來。

拾貳、願景工作坊簡介

一、何謂『願景工作坊』？

在多元化的社會裡，雖然人們的價值和利益各異，卻也面臨一些共同的問題有待解決。而解決問題，需要運用各界的知識與資訊，及社會中不同階層、立場的人們通力合作才可成功。但，對於問題解決方案的取捨，人們因利益分歧、價值有別、認知不同，對於什麼才是問題解決的「最佳方案」往往看法不一，甚至陷入衝突對立的僵局。

願景工作坊（scenario workshop）由丹麥所發展出來的一種具有審議民主精神的公民參與模式。一般來說，工作坊的參與者大約介於二十五人至三十人之間，他們分別扮演不同的社會角色，如政治人物、行政官員、科技專家、發明家與企業家。其模式是讓一般民眾、政府官員、學者專家、產業界人士以及社會團體代表，根據他們的經驗，檢視這些願景，針對共同面對的問題互相討論、交換意見並透過對話的過程，發展未來的願景尋求解決問題的方案。

因此，願景工作坊基本目標在於提出特定地區未來可能的發展，嘗試創造一個對話的空間，讓不同的人群能夠溝通、合作，發展共同行動的願景。強調收集參與者對於討論議題的看法、認知，及對於未來發展的態度與其關切的項目。藉由相互批判瞭解的過程，鼓勵提出彼此能夠接受的行動計畫，群策群力一起來解決問題。並透過不同群體的參與，讓各種知識與經驗相互交流，提升決策的品質。

二、願景工作坊進行步驟

願景工作坊是一種特別的會議形式，有一定的程序和規則。在工作坊進行之前，主辦單位會先準備「議題手冊」，淺顯易懂地介紹會議所要討論的政策議題，並撰寫一套「劇本」（scenarios），描述不同的政策方案所可能帶來的後果，讓參與者透過對劇本的批評來發展共同願景。

一般來說，工作坊的進行需要兩天時間，分作三個階段：

（1）批判、提出看法與行動計畫的具體化：在此階段中，參與者以他們的經驗、觀點與知識，來批評「劇本」所描繪的未來景象，表達他們自己對未來發展的意見。其目的在於激發想像，挖掘參與者對於未來的期待與觀點，

以協助新知識與行動計畫的產生。最後，以批判階段所產生的觀點爲基礎，形成他們對於未來發展的共同願景。

（2）行動計畫具體化的階段：與會者進一步提出如何實現願景的作法。

（3）發展行動計畫：與會者必須釐清問題並排列優先順序，指出「哪些人必須作哪些事」，才能克服障礙，解決問題，實現願景。

附錄七 2020 電子治理願景工作坊工作時程規畫

2008 年 9 月 願景工作坊時程規劃

星期一	星期二	星期三	星期四	星期五	星期六	星期日
1	2	3	4	5	6	7
	第三次執委會					
8	9	10	11	12	13	14
◦第十次籌備會議 ◦邀請名單第一波確認 ◦線上報名系統開始運作 ◦海報定稿	◦專題演講投影片定稿 ◦海報送印 ◦聯絡NPO聯合網	◦海報印製完成與寄送 ◦確認主持工作會議時間	◦世新場地確認 ◦工作人員名單確認 ◦我的E政府與研考會宣傳網頁完成	◦電子治理國際研討會		◦中秋節
15	16	17	18	19	20	21
◦第十一次籌備會議 ◦議題手冊定稿 ◦議程細流定稿 ◦聯絡各社大	◦議題手冊定稿 ◦第四次執委會	◦政大開學 ◦議題手冊送印 ◦議程海報送印		◦計畫期末報告	◦公民報名截止 ◦抽選公民並聯絡中選者 ◦寄發議題手冊 ◦接駁巴士確認	
22	23	24	25		27	28
◦第十二次籌備會議 ◦主持人工作會議 ◦製作桌牌與名牌 ◦新聞稿發佈		◦與會者和貴賓出席確認		◦行前會議與場地佈置	願景工作坊Day1	願景工作坊Day2
29	30	10 月 1 日	2	3	4	5
、願景工作坊結果整理						

附錄八 2020 電子治理願景工作坊籌備會議歷次會議記錄

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第一次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 1 月 10 日星期四
17:30-20:00</td><td>會議地點</td><td>行新大學管理學院</td></tr>
<tr><td>出席人員</td><td colspan="3">陳敦源教授、胡龍騰教授、曾冠球教授
張鐙文</td></tr>
<tr><td>會議主席</td><td colspan="3">陳敦源 教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">李基嘉、張鐙文</td></tr>
<tr><td>會議記錄</td><td colspan="3">(一)研究計畫
1.政策回顧部分 (於白板呈現，略)
2.政策現狀評估部分
(1) 計畫呈現方式第一種是比較現狀的預算、人力、組織編制和產出。第二種是比較創新。
(2) 計劃內容包括：研究問題(一至二個)，並說明研究的方法爲何和提供文獻。
(3) 預算、人力和組織編制部份好操作化，這部份一定要做比較，用一些數據分析來做兩國產出的比較。創新部份去搜集文獻找出指標，焦點放在 G to C 或是 C to G 上做了那些創新，地方政府(台北市和首爾)也要加入創新部份的探討，找出兩者最好的指標出來比較。
(4) 以我國和韓國都有的全國性政策來做比較，最好是找一樣的政策，可多列幾個政策來取得比較的交集；如市長信箱。比較完後開始焦點座談。
(5) 預算人力組織編制轉到題目一；創新轉到題目二，再想辦法和研究架構圖做連結。
陳敦源教授
1.目前主要負責統整研究計劃之緣起、目的、文獻回顧、研</td></tr>
</table>

究問題及方法

曾冠球教授

1.目前主要是負責整理歷史的發展過程；文獻回顧是過去相關的文獻和政府的文獻，回顧的背景面向可包括行政機關的擴散和科技的發展。也可以訪談的方式用滾雪球的方法，從垂直跟水平來做比較，但要在方法中交代。做初步的資料搜集就好並說明要怎麼做和爲何很重要即可。

2.訪談戶政方面可以找信義區區長張金鎮；辦公室自動化可以找台北大學企管系的陳銘薰老師和郭耀昌老師及碩博士論文；但在專業名詞的使用上可能會有差異。

胡龍騰教授

1.目前主要是負責政策現狀的評估，要包括過去和現在的政策都要。不用搜集新的東西，讓現狀能鋪陳出來就好。

初步研究架構圖(未定)

	歷史	現狀	未來
中央			
地方			
政策			

研究計劃撰寫

1.計畫緣起和目的由陳敦源教授撰寫；文獻檢閱和研究問題及研究方法由胡龍騰教授和曾冠球教授撰寫。

2.文獻檢閱和研究問題各找一至兩個問題放進去，約兩千到三千字。研究方法約一千到兩千字，總共不要超過五千字，要附參考文獻。最後由陳敦源教授來做統整。

3.1 月 20 號要交給陳敦源教授。

研究進度與時程

1.97 年 1 月至 97 年 10 月

2.97 年 1 月至 3 月準備資料與韓國學者溝通

3.97 年 5 月架構要出來

4.97 年 6 月期中報告

	5.97 年 7 月進行比較會議 **二、國際交流** 1.先用 E-mail 連絡，但不能完全用 e-mail 連絡，必須要去韓國當面溝通，大約在 3 月的時候。出國預算由陳敦源教授負責，行程和連絡事項由胡龍騰教授負責。 **三、會議時間安排** 9:00~~9:30 開場 9:30~~11:00 Overview between Taiwan and Korea (陳敦源教授) 11:10~~12:30 議題一:Vision Building (陳敦源教授) 1:40~~3:10 議題二:Local Government(曾冠球教授) 3:20~~4:50 議題三:Policy(胡龍騰教授) 5:00~~5:30 Ending **會議題目** 1.Innovation through ICTs at the local government level 2.Vision Building mechanics information of E-Gov policy comparison with Taiwan and Korea **四、研究預算** 1. 主持費每個月 1 萬元 2.助理 1 人，每個月 5 千元 3.臨時工資 6 萬元 4.韓國學者費用 1 人 3 萬，共 9 萬，住宿最多可住 3 天，1 人 1 萬 5 千元，共 4 萬 5 千元 5.會議費用 10 萬元 6.電腦耗材每人三萬元 7.文具紙張每人一萬五千元 8.整理資料的費用 1 人每小時 1 千元左右 9.飛機票 1 萬多元(7 月旺季) 10.焦點團體一場約 8 千，場地學校免錢，5 場共 4 萬。找實務界、學界跟商界、資策會的人

2020 台灣電子治理願景工作坊 第二次籌備會議會議記錄			
會議時間	民國 97 年 6 月 18 日星期四 19:30-21:00	會議地點	國立政治大學 271132 教室
出席人員	陳敦源教授、胡龍騰教授、曾冠球教授 陳序廷、李基嘉、梁芳瑜		應出席：6 人。 請假：0 人。 實到：6 人。
會議主席	陳敦源教授		
會議記錄	陳序廷		
會議記錄	一、陳敦源老師的專任助理呂季蓉（小季）協助本案報帳事宜，先向盈秋確認願景工作坊所需預算（35 萬）來源。 二、**願景工作坊預備會議暨培訓講習事宜：** (一) 日期：8/29（五)。 (二) 地點：政大行政大樓七樓會議廳（校內教師可無償借用)，待呈報中心與研考會確定後由序廷申請場地借用。 (三) 參與對象中「各地方政府於電子化政府業務之承辦人員各一名」需再向確認爲何單位（資訊還是研考？）之人員較適宜，範圍再精確一些。 (四) 可對前來的中央部會以及地方政府官員進行問卷調查。 (五) 經費部分講師費改爲 2,000 元/1 節，主題三之講師爲陳敦源老師不領講師費。 (六) 公務員出席可申請公差不需領交通費。 (七) 經費有多的部分挪到影印與印刷費加強行銷。 (八) 請陳敦源老師向林國明老師借二代健保規劃中願景工作坊的錄影資料。 (九) 由助理們發展出劇本後由三位老師修改。 (十) 規劃執行由序廷主理協同其他助理負責。		

	(十一)預算共 15 萬。 三、**願景工作坊事宜：** (一) 日期：9/27（六）、9/28（日）。 (二) 地點：世新管院 6 樓。 (三) 招募人員組成及人數改爲總人數 30 人，中央 7 名，地方 8 名，全國各地公民 15 名。 (四) 需由 5 位執行委員組成執行委員會召開兩次會議，費用再議，預計組成及人選爲： 1.本計劃主持人 1 位：陳敦源老師。 2.電子治理中心 1 位：宋子文執行長、朱斌妤主任、蕭乃沂副主任。 3.研考會 1 位：郭月娥高級分析師或其接任者。 4.學者 2 位：林劍秋（由陳敦源老師接洽）、黃東益。 (五) 給參與人員的可閱讀資料需在工作坊進行前一個星期寄送。 (六) 規劃執行由胡龍騰老師的一位學生主理（已考上台北大學研究所）。 (七) 可閱讀資料內容：主要爲電子治理&願景工作坊介紹，用語遣詞盡量淺顯易懂。 四、**下次開會事宜：** (一) 日期訂爲 6/24（下星期二），詳細時間待胡龍騰老師前一個會議時間確定後再訂。 (二) 討論可閱讀資料的內容、講師。 (三) 確定執委會成員。

<table>
<tr><td colspan="4">台灣 2020 電子化治理願景工作坊
第三次籌備會議會議紀錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 7 月 7 日(星期一)
17:30-19:00</td><td>開會地點</td><td>政治大學公行系
271149 教室</td></tr>
<tr><td>出席人員</td><td colspan="3">全體人數：8 人 ；應到人數：8 人；
實到人數：7 人 ；請假人數：1 人；
列席人數：0 人 ；缺席人數：1 人。</td></tr>
<tr><td>會議主席</td><td>陳敦源 教授</td><td>會議紀錄</td><td>梁芳瑜</td></tr>
<tr><td colspan="2">主席宣佈開會時間</td><td colspan="2">下午五點三十分。</td></tr>
<tr><td>主席認可
議程內容</td><td colspan="3">一、 確認執委會內容：
(一)執委會時間定案，7/16 上午。
(二)審核議程大綱。
(三)確認執委開會討論事項：
1.「願景」的確認。
2.「核心議題」的討論。
3.工作坊演練之「劇本」及議題手冊的討論。
4.講師、專家名單的確認。
5.工作坊培訓及招募人選方式的討論。

二、 願景工作坊部分：
(一)願景工作坊預備會議暨培訓講習計畫書審定。
(二)培訓暨正式會議計畫時程，暫定爲如表所擬，依時程順序進行。
(三)工作坊之招募人選，中央 7 位、地方 8 位人員的招募方式，需再確認，敦源老師希望政府二、三線的人也能派人出來參加。
(四)工作坊上課，主持人及講師建議部分，除敦源老師、龍騰老師、冠球老師負責外，將請電子治理中心朱斌妤老師以及黃東益老師、林國明老師、陳東升、林子倫老師等一同擔任。</td></tr>
</table>

	(五)宣傳部分，將與研討會商議做網站的連結。 (六)注意願景工作坊之籌備乃至進行、完成等過程，盡量將之轉化成可閱讀文件的方向，以供研究使用。 三、工作分配： (一)敦源老師商借蔣麗君老師，提供負責資訊業務之政府官員名單。 (二)執委會之主持以及說明部分，由敦源老師、龍騰老師、冠球老師負責報告。 (三)序廷確認第一次執委會開會場地部分，並且負責擬好議題初稿，交由曾冠球老師審核後完成。 (四)品如負責尋洽廠商設計文宣與布條、網頁等部分，並負責提供培訓相關資料。 (五)基嘉負責培訓講師與願景授課、專家名單。 (六)季蓉確認經費預估表單。 (七)芳瑜負責培訓招募人選方式草案擬定部分，並規劃培訓與願景之線上開會網站工作。 四、訂定下次會議時間： 下次會議地點爲本間教室，時間另 mail 通知。 五、散會。
聲明	主席: 1.對於 7/16 當日上午舉行的執委會，以不超過 2 個小時爲原則，中午則由本人請諸位執委一同用餐。 2.下次籌備會將討論願景工作坊前測、後測問卷部分，並且討論願景工作坊後深度訪談等議題。

2020 台灣電子治理願景工作坊 第四次籌備會議會議記錄			
會議時間	民國 97 年 7 月 21 日星期一　17:30-20:00	會議地點	政大 271149 教室
出席人員	陳敦源教授、胡龍騰教授、曾冠球教授 施品如、陳序廷、梁芳瑜		
會議主席	陳敦源 教授		
會議記錄	陳序廷		
會議記錄	**(一)培訓相關內容：** 1.培訓的出席文官人數不用到 100 人，100 人是包含工作人員。 2.培訓的出席文官之中必須有 10 人會接續參加工作坊，邀請時同時邀請他們參加培訓以及工作坊。 3.10 人名單的來源: (1) 曾冠球老師、(2) 陳敦源老師、(3) 洽詢朱主任、(4) 洽詢蔣麗君老師。統整後再交由李高分。 4.扣除 10 人名單外爲文官自由報名，人數上限再詢問李高分。 5.構思招募工作人員細節，來源以世新的學生爲主。 6.這禮拜內完成相關資料與文宣交給李高分。 **(二)工作坊相關內容：** 1.出席官員給予 1,600 元出席費。 2.助理主持人由芳瑜擔任。 3.工作坊的文官成員、業界與一般民眾頭銜均爲「2020 台灣電子治理願景工作坊諮詢委員」，會發放證書，並詢問李高分能否加蓋江主委的主委章。 4.工作坊的正式名稱爲「2020 台灣電子治理願景工作坊」，副標題或是文宣用語大家幫忙想。 5.邀約何處長蒞臨演講約 40 分鐘，主題爲「台灣電子治		

	理的沿革與展望」，詳細內容由陳敦源老師構思。 6.尋找企業界對電子化政府的願景案例，並尋找具相關內容的影片。 7.找出議題的爭議點(要有反面表述)，可加入能源、環保、信任等之概念，訂定議題名稱。 8.寫工作坊介紹、議題說明，下一次執委會要有可閱讀資料草稿給執委。 9.請執委提供業界及 NPO 名單各 8-10 人，業界的類別可分爲軟硬體、網路、傳播媒體、產業方向（例如資策會）、或請黃朝盟老師師母。 10.公民要招募無網路經驗者，報名表的基本資料要有性別、教育程度、年齡、通訊地址、聯絡電話、網路經驗(使用頻率，從數位落差的問卷找)、如何得知報名訊息、參與動機。我們的聯絡資訊問小季學姊，請她再申請一個本案專用的 email、傳真電話寫政大公行系的。 11.招募管道：(1) 我的 E 政府、(2) 社大、(3) 社區發展協會。以及善用各種網路管道各社大訊息版、BBS 等。 12.住宿旅館比價，先探詢景美快樂旅社的價格並場勘。 13.住宿要有兩位工作人員連同住宿。 14.參與者的出席費改爲 1,600 元。 15.主辦單位爲行政院研究發展考核會，承辦單位爲電子治理中心，協辦單位爲政治大學公共行政學系、世新大學行政管理學系、淡江大學公共行政系。 **(三)工作分配：** 1.詢問朱主任與蔣麗君老師文官名單：陳敦源老師。 2.何處長的演講題目與大綱：陳敦源老師。 3.請朱主任幫忙詢問宋副主委是否能出席工作坊致詞：陳敦源老師。 4.前後測問卷：胡龍騰老師。 5.電子治理的定義：曾冠球老師。（向朱老師要資料給曾

	老師參考） 6.電子治理議題的爭議點構思：三位老師（兩個正面一個反思）。 7.準備要給李高分的資料、文宣：各助理。 8.撰寫工作坊介紹、議題說明：助理。 9.諮詢委員注意事項 2 頁：序廷。 10.蒐集 IBM、Micro 的願景案例：序廷。 11.向電子治理中心索取電子治理的相關資料：序廷。 12.設計海報、網頁、logo、布條：助理。

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第五次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 7 月 31 日星期四
9:00-10:30</td><td>會議地點</td><td>政大 271149 教室</td></tr>
<tr><td>出席人員</td><td colspan="3">陳敦源教授、胡龍騰教授、曾冠球教授
施品如、陳序廷、梁芳瑜、呂季蓉、李基嘉</td></tr>
<tr><td>會議主席</td><td colspan="3">陳敦源 教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">李基嘉</td></tr>
<tr><td>會議記錄</td><td colspan="3">(一)會議相關決議事項
1. 原先需要蔣麗君老師提供的中央及地方政府官員名單確定取消。
2. 願景工作坊的授課專家邀請林子倫老師，由胡龍騰老師幫忙聯絡，品如負責邀請。
3. 願景播放影片的剪輯找榮志協助，內容包括正面及負面電子治理的議題決定爲以下四項，其下分別還要再列出一些子議題
(1)資訊安全的科技發展
(2)個人便利生活
(3)隱形政府/極小化政府
(4)跨部門整合
5.培訓會議也要做問卷的前後測，以了解與會人員在培訓前後對民主和電子化政府的認知。
6.海報及文宣格式的相關修改內容已在會議中完成。培訓及願景工作坊的海報與 DM 要做出明顯區隔，避免讓報名者產生混淆。培訓海報中政府官員的報名人數格式，可詢問電子治理中心的盈秋過去相關活動的邀請格式。海報中的電子治理中心不用加台灣。
7.向李國天高分再次確定報名網頁的協助事項，最好是能直接跟研考會的協力廠商接洽。
8.由胡龍騰老師向李國田高分確定以下事項</td></tr>
</table>

	(1)培訓會議是否能作爲與會官員的學習點數的認證 (2)參與培訓會議官員的報名方式，是要採自由報名還是全國及地方各部會(約 60 人)單位推派一名代表(包括 10 人口袋名單) (3)向何處長確認演講和推薦與會名單(別剛好 10 人) (4)是否能提供相關住宿的協助或資訊 9.由品如向何全德處長報告目前工作進度，並向何全德處長拿與會官員的推薦名單(不要剛好 10 人)。 10.培訓及願景工作坊的主持人、協同主持人及工作人員(盡量以世新學生爲主)快確定，最好在報名結束前完成。 11.培訓會議的講習主題二─電子治理與審議式民主之聯結，由陳敦源老師負責授課。 12.培訓會議的願景工作坊介紹由胡龍騰老師負責授課。 13.會議地點以世新大學爲優先選擇。 14.參與培訓的政府官員不用補助交通費。 15 下次會議時間爲：97 年 8 月 4 日星期一 下午 5:30。 **(二)下次工作進度** 1. 序廷:找陳老師需要的影集。 2. 基嘉:a.五籌會議紀錄 b.再尋找世新附近的住宿地點，並寫 mail 給各位老師告知 c.修改給諮詢委員的說明，並增加願景工作坊活動內容。 3.芳瑜:a.第二次執委會會議紀錄 b.網站架構與維護。 4.季蓉:詢問公務員差旅費的相關規定，包括交通費及住宿費。

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第六次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 8 月 18 日星期一
17:30-19:30</td><td>會議地點</td><td>世新管院大樓
M532</td></tr>
<tr><td>出席人員</td><td colspan="3">陳敦源教授、曾冠球教授
施品如、陳序廷、李基嘉</td></tr>
<tr><td>會議主席</td><td colspan="3">陳敦源 教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">陳序廷</td></tr>
<tr><td>會議記錄</td><td colspan="3">(一) 會議相關決議事項
1.公文不附海報由我們自己寄。
2.培訓的線上報名系統取消報名要記錄名單與理由。
3.培訓完畢授與結訓證書，英文名字當天頒證前發單子讓參與者自己填寫。
4.TEG 的網頁議程上要附 pdf 檔，順便附上點選專題演講議程可下載文件之功能。
5.閉幕式不舉行摸彩，重點爲發問卷與頒發證書不要拖太久盡量早點結束。
6.培訓結束當天要召開檢討會議。
7.陳老師洽問 TEG 是否有研討會用的袋子讓我們在培訓與願景工作坊使用。
8.簽到單早午各一次，閉幕式以名牌換取證書與餐盒。
9.主題一的備案人選爲曾冠球老師。
10.胡龍騰老師說明主題三時順便介紹主持人。
11.當天盡量找世新廣電或傳播科系的學生幫忙拍照，最後大合照在管院五樓的布告欄前進行，事後將所有照片 po 上 TEG 網站讓參與者自行下載。
12.讓工作人員穿上世新的背心，主持人的掛牌要有特殊顏色以便辨別。
13.邀請世新校內貴賓徐仁輝院長於開幕式接在何處長後致詞。</td></tr>
</table>

	14.第一場茶敘餐點每種要先預留四分之一給第二場。 15.本週三 8/20 演講資料要送印。 16.下禮拜籌備會議討論前後測問卷定稿。 17.培訓停車問題，確認世新第二停車場是否組約已到期，受訓者能否停在考試院停車場。 18.資訊主管名單照縣市資訊化程度排名每八名爲一個單位，高中低各邀三個。 19.下次執委會前（9 月初）先將相關資料 email 給各執委請他們給意見。 20.工作坊的報名方式要多元。 21.核心議題討論標題與順序修改，8/22（五）交劇本初稿約 1500 字 (1)便利生活與虛擬世界。 (2)個人資安與科技發展。 (3)跨域治理與整合服務。 (4)全民政府與優化民主。 22.8/23（六）下午 1:00 於世新大學管理學院大樓 M404 教室召開培訓會前工作會議，當天胡龍騰老師會到場說明培訓當天注意事項。 23.8/28（四）培訓前一天要麻煩執行助理們留下佈置會場，會再通知時間與地點。 **(二) 下次工作進度 8/22(五)初稿** 1.從台北車站到世新的捷運路線、公車與站牌資訊：序廷 2.世新附近的住宿資訊：基嘉。 3.核心議題一：品如。 4.核心議題二：胡龍騰老師、基嘉。 5.核心議題三：曾冠球老師、芳瑜。 6.核心議題四：陳敦源老師、序廷。

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第七次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 8 月 25 日星期一
17:30-19:30</td><td>會議地點</td><td>世新管院大樓
M532</td></tr>
<tr><td>出席人員</td><td colspan="2">胡龍騰 教授、曾冠球 教授
施品如、陳序廷、梁芳瑜、李基嘉</td><td>應出席：8 人。
請假：2 人。
實到：6 人。</td></tr>
<tr><td>會議主席</td><td colspan="3">胡龍騰 教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">梁芳瑜</td></tr>
<tr><td>會議記錄</td><td colspan="3">一、上次會議決議事項回覆
(一)培訓報名現況：
各助理回報，各機關接收公文單位顯非資訊部門，多有送至人事室，甚至統計室、稅務處室的狀況，且因公文上只寫了「歡迎參加」的敘述，多有機關因事務繁忙直接將公文批簽完結，報名狀況並不踴躍。胡老師補充，因公文上的限制，導致各單位回覆不如當初所預期，但請各助理不要因此有壓力。

(二)確認培訓事項（細流、前後測問卷、可閱讀資料）：
胡老師於前測問卷中增加了 5 題，確定無誤；講演部份 PPT 資料也已備妥，另調整大會午餐時間由 11 點 30 調至 11 點 50，以防演講時間過長超出時間表。

(三)確認願景核心討論議題與劇本：
劇本部份已初步完成，本日稍晚將會由陳老師做最後核定。

(四)確認願景進度（遴選名單、議題手冊、宣傳）：
名單方面，業界以及 NPO 較缺乏，執委尚未提出完整建議名單，需加強 PUSH 執委，而名單提出確認後，將由老師</td></tr>
</table>

	們親自打電話邀請，不發公文。 **二、相關討論事項：** (一)9 月 10 日韓國學者將來台參與研討會發表，胡老師建議支援對韓國學者的招待，確定由三位老師接風，請助理機動協助；並做 9 月 11 日的行程規劃，暫定招待台菜，餐廳另議。 (二)培訓以及工作坊活動當日有四台攝影機，必須架設妥當，並決定其中一台可以即時上傳轉錄的攝影機，架設於「政府組」所在教室。 (三)預支經費問題，由於活動經費尚未撥款，於是先行向曾老師提借 1 萬 4 千元,以做飯店住宿訂金及採買雜支用。 (四)第三次執委會議時間與討論準備事項： 第三次執委開會時間諮詢狀況，目前剩資策會林劍秋顧問尚未回覆，先就各執委以及老師們時間，將定於 9 月 2 日下午，下午 4 點，召開第三次執委會議。

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第八次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 9 月 1 日星期一
17:30-20:00</td><td>會議地點</td><td>世新管院大樓
M532</td></tr>
<tr><td>出席人員</td><td colspan="2">陳敦源 教授、胡龍騰 教授、曾冠球 教授、朱盈秋、林儀郡、呂季蓉、施品如、陳序廷</td><td>應出席：10 人。
請假：2 人。
實到：8 人。</td></tr>
<tr><td>會議主席</td><td colspan="3">陳敦源 教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">陳序廷</td></tr>
<tr><td>會議記錄</td><td colspan="3">(一) 願景工作坊相關決議事項
1.第一、第二天的議程重新安排。
(1)開幕式讓參與者自我介紹。
(2)每場茶敘改爲 10 分鐘。
(3)每場演講改爲 40 分鐘。
(4)加入陳敦源老師的專題演講，主題與培訓同爲「電子治理與審議式民主」，時段安排爲 11:30-12:10。
(5)第一天下午要留半小時讓參與者閱讀資料與劇本，時段安排爲 13:00-13:30。
(6)確認第二天議程是否漏掉「好點子說明」（與其他活動對照）。
2.報名截止日由預定的 9/15 延長五天至 9/20。
3.宋副座的投影片目前已知宋副座會自行準備，投影片格式與內容請盈秋幫忙聯繫，希望 9/9 出來，內容能讓與會者對台灣電子治理的沿革與未來規劃有所了解，特別是官方觀點。
4.目前議題手冊內並未提及工作坊的操作介紹，從工作坊的計畫書內加入相關內容。
5.議題手冊內要補上過去台灣這方面的發展，以及世界各國的做法，這部分由陳敦源老師提供 paper 由曾冠球老</td></tr>
</table>

	師節錄整合。 6.在這週內將議題手冊初稿給林子倫老師參考，並詢問林老師是否有要在演講中播放有關願景工作坊的影片。 7.劇本一、二與劇本四之間有部分重疊，再行統合，e-voting 的議題均挪至劇本四呈現。 8.議題手冊格式先統一，放上部分圖片，再對照之前的活動手冊檢查未盡周延之處。 9.索取青輔會願景工作坊的 DVD，陳敦源老師演講可撥放部分內容。 10.培訓預算結餘約七萬多元，朱主任表示結餘可全數挪至願景工作坊使用。 11.參與者住宿改爲單人房，房間由原先預訂的 15 間多訂至 25 間。 12.工作坊當天主持團隊均穿著紫色 polo 衫，分組會議的好點子海報格式要統一，貼點的貼紙要改用最大的。 13.詢問工廠海報印製好後直接包裝統一寄送社大的問題，海報寄送要附上報名表，另李高分表示可協助將活動訊息放置我的 E 政府首頁。 14.主持人對電子治理的議題要熟悉，主持人與助理主持人的協調問題以盡量不換人爲原則，若兩人溝通或默契不佳則由主持人自行尋找助理主持人搭擋。 15.與會者邀約由三位老師分工。 16.胡龍騰老師擬一份說明與邀約的傳真信函。 17.確認兩位參與中港大排的願景主持人能否主持工作坊。 18.臨時聘用兩位助理在這個月內協助工作坊的籌畫與執行。 (1)政大：黃重豪。 (2)世新：黃榮志。

	(二)下次工作進度 1.9/5（五）海報、議題手冊初稿完成。 (1)封面設計、格式統一、放圖片：小品。 (2)劇本統整：序廷（明早先寄給陳老師修改）。 2.索取青輔會 DVD：序廷。 3.聯繫林子倫老師：小品。 4.確認兩位參與中港大排的願景主持人出席狀況：小品。 5.住宿房間加訂：基嘉。 6.與會者邀約分工： (1)政府：曾冠球老師。 (2)業界：胡龍騰老師。 (3)NPO：陳敦源老師。

2020 台灣電子治理願景工作坊 第九次籌備會議會議記錄			
會議時間	民國 97 年 9 月 8 日星期一 17:30-21:30	會議地點	世新管院大樓 M532
出席人員	陳敦源教授、胡龍騰教授、曾冠球教授 陳序廷、梁芳瑜、李基嘉、黃榮志		應出席：8 人。 請假：1 人。 實到：7 人。
會議主席	陳敦源教授		
會議記錄	梁芳瑜		
會議記錄	**一、願景工作坊進度：** (一)九月工作進度表確認。 (二)海報確認並送印；序廷已於晚間七點當時與廠商確認完畢。 (三)議題初稿審核，煩請三位老師確認。 (四)活動當日中心可提供人員須穿著的背心，並列爲必要要求。 (五)工作團隊訂於 9 月 22 召開十二籌會議時，同時舉行對「主持人群」做一電子治理的知識教育。 (六)確認要給十位官員的資料以黑白列印先行寄送；彩印正式版 時活動當天領取。 (七)公民報名截止爲 9 月 20 日，決議報名截止當日即刻把所有會議資料寄發送出。		

	(八)暫定 9 月 16 日再第四次執委會議。 (九)BBS 宣傳擬用「活動看板」的醒目方式，篩選適合的討論版後，再行廣告；由芳瑜負責及分配。 (十)陳敦源老師提醒：邀約或接受電話報名時，關於 NPO 的部份要注意確認與一般公民報名分開。 (十一)各老師的邀約進度最後會交由大會(序廷)統一並做最後回應。 (十二)朱老師協助邀約的部份則與曾老師一同匯整。 (十三)新聞稿發文由芳瑜負責撰寫，建議結合時事以及加入活潑或具爭議可討論的素材以引起注目利宣傳。胡老師補充：可以先前廣爲報導的「上網結婚登記」新聞結合。 (十四)住宿訂房確認以單人房爲主，雙人房爲輔，駐點協助人員以「男男」或「女女」雙人搭配爲宜。 (十五)手冊印製數量決議以 80 份爲量，若全彩列印則下調改印製 60 份；以初估 80 頁一份請廠商報價。 (十六)宋副主委的題目是否還有更動？請序廷與中心確認或做修改。 (十七)設法找五個當前最新的資訊或數位產品的相關研發，以之爲題材，放入「何爲電子治理」章節，並加入相關電影的介紹，以利活動參與人員發想。陳老師舉例，

	如「部落格是什麼」的發展始末；陳老師則可提供「NGM」的題材，以結合成爲未來科技與電子治理的課閱讀資料的豐富度。 (十八)工作人員名單確認無誤；陳老師認爲女士優先，建議把女性工作人員放名單之前。 (十九)下次會議將一併討論期末報告架構的確認。 **二、助理工作事項討論：** (一)進度表部分，建議把 9 月 23 日的「製作桌牌與名牌」與前一日(22 日)召開十二籌會議結束後一併完成。並補充補上中秋節時程。 (二)活動當日攝影機腳架借用的數目，確認爲五支。 (三)24 日的進度的貴賓與人員出席確認，分配給各位助理協同於活動三天前電話確認。 (四)26 日行前會議時，將請工作人員一起場佈，以增加臨時工作人員的熟悉度與團結度。 (五)助理工作分配： 1.序廷加入與確認活動所有報名人聯繫事項。 2.基嘉加入飲食與訂餐、停車未確認事項；並與榮志負責管理所有世新臨時工作人員的臨行訓練，以及提出器材清單。 3.芳瑜負責主持與活動議程細流編制以及 BBS 設廣告看板的。

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第十次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 9 月 15 日星期一
17:30-20:30</td><td>會議地點</td><td>世新管院大樓
M532</td></tr>
<tr><td>出席人員</td><td colspan="2">陳敦源教授、胡龍騰教授、曾冠球教授
陳序廷、黃榮志、李基嘉、黃重豪</td><td>應出席：8 人。
請假：1 人。
實到：7 人。</td></tr>
<tr><td>會議主席</td><td colspan="3">陳敦源教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">黃重豪</td></tr>
<tr><td>會議記錄</td><td colspan="3">(一) 願景工作坊相關決議事項
(1) 議題手冊黑白影印 40 份，彩色影印 50 份，彩色影印部分若經費充足可再追加。
(2) 會場發放彩色議題手冊，並將投影片附於附錄。
(3) 於手冊外另製作一份交通指引。
(4) 告知與會者會場地下室保留 10 個免費停車位，先到者優先使用，但國家考場附近仍有車位。
(5) 由於目前報名的公民代表性不足，請各位盡量尋找身邊具草根性，或地方上的意見領袖，以增加普羅大眾的代表性。
(二) 工作分配
(1) 前言（約 2500 字）（陳老師）
(2) 理論（約 14000 字）
a. 電子治理與願景建立（2000 字）（陳老師）
b. 參與與願景工作坊（2000 字）（陳老師）
c. 外國趨勢（5000 字）（陳老師）
d. 國內趨勢（5000 字）（曾老師）
e. 跨國比較（5000 字）（胡老師）
(3) 操作（15000 字）
a. 議程（確認人員）（7000-8000 字）：理論、國內、國外（文獻、中韓）</td></tr>
</table>

	b. 願景工作坊設計與執行（7000-8000 字）（胡老師、曾老師） (a)緣起 (b)程序 (c)執行 (d)結果 (4) 結論與建議（胡老師、曾老師）

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第十一次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>97 年 10 月 1 日星期三
10:30-12:00</td><td>會議地點</td><td>世新管院大樓 M611</td></tr>
<tr><td>出席人員</td><td colspan="2">陳敦源 教授、胡龍騰 教授、
陳序廷、黃榮志、黃重豪</td><td>應出席：8 人。
請假：3 人。
實到：5 人。</td></tr>
<tr><td>會議主席</td><td colspan="3">陳敦源 教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">陳序廷</td></tr>
<tr><td>會議記錄</td><td colspan="3">(一) 願景工作坊補辦決議事項
(1) TEG 再補助十萬元於補辦活動。
(2) 補辦日期訂爲 10/18（六）。
(3) 地點以世新管院爲優先，備案爲政大綜合院館。
(4) 補辦出席費 1,000 元，只提供前一晚的住宿。
(5) 當天活動結束後優先訪談中南部的參與者。
(6) 前一次的出席費 2,000 元以現金袋寄出，附上補辦的說明信函，附上活動議程與願景整理，署名陳敦源老師。
(7) 現金袋寄出後以電話通知受訪者，告知錢已寄出、活動補辦訊息、補辦出席費另計、住宿及交通費比照辦理。
(8) 提醒參與者攜帶議題手冊，活天當天另預備十餘冊黑白本供索取。
(9) 下週一晚上再開會。
(二)工作分配
(1) 調查世新館院場地借用狀況：榮志。
(2) 調查政大綜院場地借用狀況：序廷。
(3) 確定 10/17 中信空房間數：基嘉。
(4) 聯繫主持人：序廷。
(5) 錄音逐字稿架構整理：榮志。
(6) 說明信函草擬：序廷。
(7) 現金袋寄發：序廷。</td></tr>
</table>

2020 台灣電子治理願景工作坊 第十二次籌備會議會議記錄			
會議時間	民國 97 年 10 月 6 日星期一 17:30-19:30	會議地點	世新管院大樓 M310
出席人員	陳敦源教授、胡龍騰教授、曾冠球教授 陳序廷、梁芳瑜、李基嘉、黃榮志		應出席：8 人。 請假：1 人。 實到：7 人。
會議主席	陳敦源教授		
會議記錄	梁芳瑜		
會議記錄	一、願景工作坊補辦事項： (一)活動結餘與補辦預算整理回報： 1.住宿費最大化預估：30 名*1800 元/晚=54000 2.交通費：比照上次活動補助規定。 3.接駁：前一晚預先住宿者，以「計程車」補助置場地，不另租用巴士接駁。 4.地點：決議以世新「通識大樓」爲補辦場地。 5.上次給予與會者的津貼目前只餘一位政府官員因公差在外連絡不上，其餘皆已確認並以限時掛號現金袋發放完畢。 6.本次停車場位置與上次場地不同，通知時請務必特別說明。 7.交通停車規劃，請助理榮志負責，並負責工讀生規劃分配。 8.住宿因中信飯店已無房間，要住宿者本次預訂「快樂旅社」。 (二)願景工作坊研究進度： 1.逐字稿以及後續訪談謄稿，決定外包處理，須盡快清算計劃本體結餘，才可規劃。 2.對與會者的後續訪談，於願景工作坊活動完畢後另約		

	時間進行，需對與會者同時告知；決議訪談不另再給費用。 3.DV 母帶將於今晚同時轉帶完畢。 (三)研究案討論： 1.陳老師： (1)明年美國 ASPA 論文發表已被接受。 (2)service 本身是有一個總量上限的，所以，用商業的眼光來計畫 e-service 可能是有問題的？ (3)爲什麼總有人要 face to face 做申辦？ (4)如果國家政策網路智庫不以 service 的總量來看，而是以民眾 empowerment 參與政策推出來看，又如何？ (5)探討放入「e」到底是一種 technologic、還是一種管理創新？ (6)SEXY 的研究題目，很重要。 2.胡老師： (1)系統平台的整合爲什麼會慢？是不是與官僚的抗拒有關？基於其既有習慣、行爲、利益等？是否可以實證？ 3.曾老師： (1)「e」是不是改變了組織？會改變組織嗎？

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第十三次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 10 月 13 日星期三 17:30-20:00</td><td>會議地點</td><td>世新管院大樓 M301</td></tr>
<tr><td>出席人員</td><td colspan="2">陳敦源教授、胡龍騰教授、曾冠球教授
陳序廷、梁芳瑜、李基嘉、黃榮志</td><td>應出席：8 人。
請假：1 人。
實到：7 人。</td></tr>
<tr><td>會議主席</td><td colspan="3">陳敦源教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">陳序廷</td></tr>
<tr><td>會議記錄</td><td colspan="3">願景工作坊補辦決議事項
(1)10/18 晚上提供餐盒。
(2)助理主持人缺先問小品再請家華幫忙。
(3)當日訪談台北縣市以外的參與者，老師跟助理全部下去訪談，不足的人數再找工讀生幫忙。
(4)訪談場地爲通識大樓的七間教室。
(5)跟系辦借錄音筆，另也請訪談者自備錄音筆。
(6)訪談者的出席費當日訪談完再發放。
(7)星期五舉辦行前會議、主持會議以及訪談說明。
(8)北縣市的後續訪談部分平均分配給三位老師，由助理執行。
(9)確認通識教室的設備。
(10)最後會產出 36 個行動方案。</td></tr>
</table>

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第十四次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 10 月 20 日星期一
17:30-21:30</td><td>會議地點</td><td>世新管院大樓
M310</td></tr>
<tr><td>出席人員</td><td colspan="2">陳敦源教授、胡龍騰教授、曾冠球教授
陳序廷、梁芳瑜、李基嘉、黃榮志、
黃重豪</td><td>應出席：8 人。
請假：0 人。
實到：8 人。</td></tr>
<tr><td>會議主席</td><td colspan="3">陳敦源 教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">梁芳瑜</td></tr>
<tr><td>會議記錄</td><td colspan="3">一、序廷報告：

1.10/18 願景工作坊當天所進行的訪談，人數共計 18 位，受訪者人名漏登記的那位，應是張常昌；其餘參與者還剩居住台北縣市者 23 位須訪談。
2.逐字稿與後續訪談，陳老師指示也切割成三等分來分配，並且請序廷先統一訂好格式再發包；逐字搞必須是詳盡包含訪問者與受訪者兩者對話的。
3. 請領單據請一定要有「店章」；可沒有統編但不能漏店章。

二、陳老師指示：

1.訪談與逐字搞的工讀費用，從八萬元的支出去使用。
2.分配名單上請序廷載明：電話、地址；名單資料給助理就好，不需再傳給老師。
3.議題手冊部份，再加印 20 本，給予(1)台大館藏，(2)電子治理中心，(3)老師，(4)助理們留存；加印時請注意可能侵權的圖案。
4..願景工作坊兩天的活動，擬作成影片，看是否能放在中心網頁，可供宣傳點閱。
5.請榮志詢問世新廣電等系所，是否有可合作班我們將活動剪接成光碟的；目標是成爲類似「華視新聞雜誌」般的節目影片。</td></tr>
</table>

	6.工作坊第二天只做上午場的逐字搞發包，比照 9/27 第一天的作法。 **三、老師討論：** 1.是否有計畫出成書？是否有此心？如果有，則擬將研究報告再做修正。 2.出版是否涉及版權？屬研考會或是屬於老師自身？ 3.以本次觀之，劇本的演練的確重於願景建置本身。 4.自問：找公民進來的理由是什麼？ 5.針對期末報告，「跨國比較」部分基本上不要再動，而是加入「國內」部分的料進來。 6.針對審查意見的回應： (1)確定一下「蚊子館」在國外是否有類似的說法或名詞？ (2)研究報告中，需要再檢查；EX 我們沒有做民調，所以這部份要刪掉，而以 9/27 與 10/18 的前後測問卷來對照取代。 (3)序廷負責把研究報告中的「附錄」檢視並再做完整。 (4)11 月底前，把所有的研究帳目都報完。

<table>
<tr><td colspan="4">2020 台灣電子治理願景工作坊
第十五次籌備會議會議記錄</td></tr>
<tr><td>會議時間</td><td>民國 97 年 11 月 8 日星期三
17:30-20:00</td><td>會議地點</td><td>世新管院大樓
M511</td></tr>
<tr><td>出席人員</td><td colspan="2">陳敦源教授、胡龍騰教授、曾冠球教授
陳序廷、梁芳瑜、李基嘉、黃榮志</td><td>應出席：8 人。
請假：1 人。
實到：7 人。</td></tr>
<tr><td>會議主席</td><td colspan="3">陳敦源教授</td></tr>
<tr><td>會議記錄</td><td colspan="3">李基嘉</td></tr>
<tr><td>會議記錄</td><td colspan="3">一、序廷報告：

1.採買單據超過 1 萬元，要向店家開估價單。
2.截至本次會議，已經報出去的帳目確認。

二、結案報告討論：

1.把會議討論出的願景用文字方式陳述出來並和願景整理表放在一起。
2.由曾冠球老師負責補充研究方法的內容
3.結案報告第一章由陳敦源老師負責。
第二章文獻回顧的 1.2.3 節由陳敦源老師負責，4.5 節由曾冠球老師負責，並加上一個小結。
4.第三章由胡龍騰老師負責，找出行動方案中
(1)哪些是政府過去已經做過的，哪些是沒有做過的。
(2)政府作的優先順序爲何。
(3)討論出來的行動方案中，有哪些是比政府現有更好的。
5.陳敦源老師建議，要讓政府資訊相關單位能以去閱讀此本白皮書，並說明要用什麼方法來做。</td></tr>
</table>

	三、助理工作： 1.序廷負責 (1)分析願景工作坊，做一個執行評估 (2)抓問卷中的不同面向用 SPSS 做前後測的分析，如知識等…組別要分爲政府組、業界組、NPO 組、公民組和全部與會者。並把問卷最後一題最質化分析。 2.芳瑜負責 (1)重新整理第一天產出願景、貼點前行動方案和貼點後行動方案的表格，並交給胡龍騰老師。 3.基嘉負責 (1)做結案報告的附錄，包括美國、韓國和台灣的電子治理相關法案，2020 台灣電子治理願景工作坊的相關資料和訪談的逐字名單。

附錄九 2020 電子治理願景工作坊執行委員會歷次會議記錄

<table>
<tr><td colspan="4">台灣 2020 電子化治理願景工作坊
會議紀錄</td></tr>
<tr><td>會議名稱</td><td>「台灣 2020 電子化治理願景工作坊」第一次執行委員會</td><td>會議時間</td><td>民國 97 年 7 月 16 日
星期三</td></tr>
<tr><td>主席</td><td>陳敦源 教授</td><td>開會地點</td><td>政治大學公行系
271149 教室</td></tr>
<tr><td>會議紀錄</td><td colspan="3">李基嘉</td></tr>
<tr><td colspan="4">出席人員

執行委員：
財團法人資訊工業策進會/林劍秋 顧問規劃師、研考會/李國田 高分電子治理中心主任/朱斌妤 教授、政治大學公共行政學系/黃東益 教授
政治大學公共行政學系/陳敦源 教授、世新大學行政管理學系/胡龍騰 教授
淡江大學公共行政學系/曾冠球 教授

列席人員：施品如、陳序廷、梁芳瑜、呂季蓉、李基嘉</td></tr>
<tr><td colspan="2">主席宣佈開會時間</td><td colspan="2">上午十點。</td></tr>
<tr><td colspan="2">主席認可議程內容</td><td colspan="2">一、執委會確認內容
(一)培訓與願景工作坊的主持人確定爲陳敦源 教授。

二、培訓會議相關確認內容</td></tr>
</table>

	〈1〉參與培訓的政府官員 10 人與願景工作坊相同，其他採自由報名方式，均不領出席費。 〈2〉培訓會議的名稱要確定，由工作團隊負責確認。 〈3〉培訓會議的地點改爲世新大學，時間不變。 〈4〉培訓會議的授課主題一，改以介紹台灣電子化政府發展過程爲主軸，並試邀請研考會資訊管理處何全德處長爲主講人。 〈5〉培訓會議議程下午分組模擬操作，仍須討論分成幾組較爲恰當。 **三、願景工作坊相關確認內容** 〈1〉參與願景工作坊的政府官員修正爲 10 人，由執委會委員共同提出名單，確定後發文邀請參與，名單要在第二次執委會之前出來，交由李國田高分呈報上級排序決定。後續要有兩頁的說明。 〈2〉出席願景工作坊的政府官員可領出席費，1000 元過低，最後金額尚未確定。 〈3〉願景工作坊的主題要加以確定，最好是疑問性的方式，後續子議題要具爭議點存在。此部分須執行會委員與老師們以 E-mail 加以聯繫確定。 〈4〉議題手冊有關於專業的東西，要能讓參與的民眾確實瞭解。 〈5〉願景工作坊則試邀請研考會副主委爲專題演講二台灣電子化治理相關政策與未來期許主講人。 〈6〉願景工作坊一般公民代表修正爲 10 人，邀請方式與條件要說明清楚。相關業界代表 10 人採邀請方式招募。 〈7〉公民招募所需的網頁廣告和行政院研考會網頁的廣告連結研考會會加以協助。 〈8〉願景工作坊開會地點仍須作確認，因爲全國性

	會議晚上須安排住宿，建議開會地點離住宿距離相近較佳。 **四、其他確認內容** 〈1〉專家與授課者名單，需執委會委員以 E-mail 加以聯繫確定。 〈2〉第二次執委會時間初定在七月底至八月初之間。
主席宣佈散會時間	下午一點。

2020 台灣電子治理願景工作坊

會議紀錄

會議名稱	「2020 台灣電子治理願景工作坊」第二次執行委員會議	會議時間	民國 97 年 7 月 31 日 星期四
主席	陳敦源 副教授	開會地點	政治大學公行系 271149 教室
紀錄	梁芳瑜	出席人員	詳見簽到表
全體人數：12 人 ；應到人數：12 人； 實到人數：11 人 ；請假人數：1 人； 列席人數：0 人 ；缺席人數：0 人。		會議類別	□ 定期 □ 臨時

主席宣佈開會時間	上午十點三十分。
主席認可議程內容	**二、 第一次執委會會議結論與討論：** (一)給予參與政府官員、業界與一般民眾的證書，由電子治理中心主任署名即可，證書是否需要中英文對照，可再討論。 (二)出席願景工作坊之政府官員、業界與一般公民之出席費用原訂 1600，黃東益老師建議提高至 2000-2500 元，朱斌妤主任建議查閱主計法規後，或向李高分確認公務員出席費用規定，再做調整。另外願景工作坊乃在週末進行，是否給予出席費用有不同標準，請工作團隊一併確認後定案。 (三)培訓除了固定的 10 位內定政府官員外，工作人員約 20 位，另外其餘中央與地方政府官員擬訂自由報名參加的額數為 40 名。

	(四)住宿方面，因原定快樂旅社能提供房間數有限，相關的住宿地點與開會地，將增編租車交通預算，以擴大尋覓合適地點範圍；住宿地點請工作團隊商洽研考會、世新會館與考試院等有否合適場地提供而定。 (五)朱主任確定公文部份將由電子治理中心發文，請專案助理品如與中心助理盈秋照會公文細節後，與李高分確認再行文各相關單位。 (六)附件二的參與說明部份，名稱建議改成「參考資料」等較爲適當，或着文成「系列活動」較爲適宜，此部分將交由陳敦源老師修整確認後做最後定案。 (七)政府官員 10 人部份，擬請何處長提供名單。 (八)培訓之主題二演講部份，將由陳敦源老師擔任主講人；願景工作坊介紹專題則由胡龍騰老師擔任主講。 (九)執委將於下次會議討論工作坊議題與議題手冊，並且定案。 **二、散會。**
聲明	主席： 其餘事項留於下禮拜一八月四日籌備會議時討論
主席宣佈散會時間	中午十二點四十分。

2020 台灣電子治理願景工作坊

會議紀錄

會議名稱	「2020 台灣電子治理願景工作坊」第三次執行委員會議	會議時間	民國 97 年 9 月 2 日 星期二
主席	陳敦源 副教授	開會地點	政治大學公行系 271149 教室
紀錄	黃榮志	出席人員	詳見簽到表
全體人數：13 人 ；應到人數：13 人； 實到人數：10 人 ；請假人數：3 人； 列席人數：0 人 ；缺席人數：0 人。		會議類別	□ 定期 □ 臨時

主席宣佈開會時間	上午十點三十分。
主席認可議程內容	**一、 第三次執委會會議結論與討論：** （一）對於上週(8/29)願景工作坊概況說明： 1. 問卷分析尚未完成(包含前後測)。 2. 培訓成果報告書。 （二）願景工作坊議程與活動內容： 1. 開幕式縮短爲十分鐘，茶敘改爲一場，茶敘後安排十五分鐘的自我介紹時間。 2. 林子倫老師的演講加上主持人介紹，並與陳敦源老師的時間對調，調整爲第專題演講二。 3. 確認 9/27、9/28 願景工作坊的劇本。 4. 個人資安的劇本還須修改(如結婚登記之類的)。 5. 李高分建議業務與資訊相關、業務導向使用資訊工具、資訊人員是九月邀約的目標。

	6.九月十一日要確認世新的教室，場地、人員經過上周的培訓，九月底時繼續招募。主持人部分沒有問題，需替補的助理主持人更換兩名，已找到。 7.海報、運作模式未來將標準化。所有工作都必須標準化。 8.願景工作坊陳老師上課時會使用部分好萊塢電影片段來增加願景的未來感。 （三）願景授課、專家邀請進度：宋副主委、林子倫老師、陳敦源老師都已確認。 （四）議題手冊部分： 1.願景工作坊的步驟要加上流程圖和對應的培訓照片。 2.電子治理各國情形需簡化，第五大項的表格未必要放。 3.議題手冊格式須統一，參照附件三何謂「電子治理」的格式。 4.何謂「電子治理」這部分請曾冠球老師加上台灣的情形，並舉例說明，可參閱電子化政府報告書。 5.與主持人討論願景工作坊的小組所需時間，以及討論議題之數量。 6.將活動宗旨、計畫書前言放入議題手冊。 7.劇本的標題要隱藏。 8.工作人員的簡介加入議題手冊並加上執行架構。 9.主持人經歷加入 PPT。 10.將活動宣傳 POST 到 BBS 上。 （五）下周工作會報，報告邀請狀況。曾老師邀約

	政府單位時希望能全程參與。 **二、散會。**
聲明	主席: 其餘事項留於九月八日（一）籌備會議時討論
主席宣佈散會時間	下午六點四十分。

<table>
<tr><td colspan="4">台灣 2020 電子化治理願景工作坊
會議紀錄</td></tr>
<tr><td>會議名稱</td><td>「2020 台灣電子治理願景工作坊」第四次執行委員會</td><td>會議時間</td><td>民國 97 年 9 月 16 日
星期二</td></tr>
<tr><td>主席</td><td>陳敦源 教授</td><td>開會地點</td><td>政治大學公行系
271149 教室</td></tr>
<tr><td colspan="4">出席人員
執行委員：
財團法人資訊工業策進會/林劍秋 顧問規劃師、政治大學公共行政學系/陳敦源 教授、政治大學公共行政學系/黃東益 教授、世新大學行政管理學系/胡龍騰 教授、淡江大學公共行政學系/曾冠球教授</td></tr>
<tr><td colspan="4">列席人員：陳序廷、梁芳瑜、呂季蓉、李基嘉、黃榮志</td></tr>
<tr><td>主席宣佈開會時間</td><td colspan="3">下午 5 點。</td></tr>
<tr><td>主席認可議程內容</td><td colspan="3">執委會確認內容
(一)議題手冊
1.議題手冊要加上書背、專題演講的投影片要放在議題手冊的後面，並在表示在目錄上
2.林子倫老師的專題演講要設一個給我們投影片的時限
3.議題手冊中的標題要改成較好看的字體，不要用新細明體
4.議題手冊送印確定
(二)報名事項
1.林劍秋委員建議可找台東縣政府資訊處的曹劍秋先生參與本次願景工作坊
2.目前的報名情況還是欠缺公民的參與
3.星期五看報名狀況決定是否要延長開放報名的時間
4.若分組的人數已經足夠，就將自由報名系統中，是</td></tr>
</table>

	邀約來的人當作公民組，相反情況亦然。若人數真的不足，只好併組處理 5.林劍秋委員可提供能連絡到一般公民的人士 6.由數位落差輔導組織的人來找有意願參加的公民 7.業界人士的邀約可找企管系幫忙，曾冠球老師也會提供名單上的協助 8.由黃東益老師之前訪談過的村里長來幫忙找公民參加 9.後備方案是找老師教的學生來參加
主席宣佈散會時間	下午七點。

附錄十 2020 台灣電子治理願景工作坊小組討論結果

◎議題一願景一

政府組	NPO 組
1.由政府針對網路之管理與品質立法(EX：電信市場主導之問題)並調整至一般大眾能負擔之網路費用，或補助相關費用給偏遠地區，另結合企業、ＮＰＯ、各業界進行資訊教育推廣(EX：建立諮詢系統) 2.由政府成立推動小組(可採發包、民營化、公開招標方式)並結合電信業者，制定相關行動上網裝置及資訊交換平台的標準。	1.由政府部門編列預算及做規劃，建置基礎網路設備，讓光纖能到每一戶家庭；並建置都市、戶外無線網路環境，讓民眾能隨時隨地高速上網，獲取資訊，尤其離島、偏遠地區鄉鎮，更要完善整理。ＮＧＯ、ＮＰＯ也可透過向企業募款，發展爲區域性資訊提供中心，且與各縣市政府，在地教育訓練機構合作，提供教育訓練、規廣，鼓勵銀髮族及身心障礙者上網。 2.公部門補助公民每人行動電話(如：ＰＤＡ)，作爲公民接受政府訊息、查詢資訊以及回報資訊載具。達成雙向資訊回報、流通功能。 3.政府可規劃二手設備流通、交換平台、提供公部門、學校釋出舊設備(如：電腦)，並開放偏遠地區有需求單位(如：學校、ＮＧＯ、ＮＰＯ團體)申請，達到物盡其用且提供需求單位擁有充足資訊收發載具目的。

業界組	公民組
1.企業提供業界資訊平台分享，與政府平台進行部份整合。 2.政府可透過企業資源（非政府的館藏）進行合作達到資訊共享。 3.公共服務資訊的建立，應有競爭與監督機制，並採取使用者付費	1.政府須建立友善的電信環境，成立網路費率審議委員會，制定費率的上限，並創造公平競爭的獎勵投資機制與誘因以提高網路服務的品質。 2.宣傳方式是透過多元公民教育管道：(1)戲劇(大眾傳播) (2)里辦公室負責(大聲公、宣傳車) 3.爲減少數位落差情形，針對弱勢族群，政府須編列更多預算，增添設備及補並提供電腦上網學習的機會。

◎議題一願景二

政府組 1.結合地方、中央政府建立單一窗口(EX：政府網頁個人化)。訓練第一線人員或資安人員後續資料整合技術，並對其業務分類、分級(EX：對稅收稅率制定之政策)。	NPO 組 4.政府應成立高層級資訊主責單位，如:資訊部、資訊局、獨立預算、獨立人事編制，由其主責全國各資訊相關政策規劃、推行。(地方主管機管要配合) 5.政府應透過立法或行政命令發佈，破除各部門、單位隔閡，加速達成資訊整合系統，提供便民服務。(如：戶政、地政、健保局、國稅局資訊整合)，讓民眾至任一公部門均可辦理相關業務，免於奔波。
業界組 1.提供政府資訊電子影像並普及化，讓政府電子平台能夠及時傳輸訊息及回覆。	公民組 1.配合軟硬體的行動方案建置 (1)公民可透過電視、手機代替電腦介面，以遙控器或手機按鈕即可辦理相關業務。 (2)亦可透過里辦公室及便利商店使用介面。

◎議題一願景三

政府組 2.要求跨部門協商，各部會首長定期開會以利資訊流通，當災難發生時，可即時獲取各單位之資訊。 3.由政府輔導或委託政府組織成立各地服務中心，即時提供公共訊息。 4.公共服務資訊可透過交通工具系統、ＰＤＡ等媒介，由民眾自行訂閱想要的即時資訊。	NPO 組 6.政府提供不同媒介的平台提供災難、治安、交通、老人安全的資訊、即時發布、傳遞與回報。
業界組 3.企業提供業界資訊平台分享，與政府平台進行部份整合。 4.政府可透過企業資源（非政府的館藏）進行合作達到資訊共享。 3.公共服務資訊的建立，應有競爭與監督機制，並採取使用者付費	公民組 1.同３－１－１的行動方案政府須設置相關資訊平台，並可由公民設定往後需要收到資訊的類型(如交通)，方式(如簡訊或ｅ－ｍａｉｌ等)。

附錄十一 2020 台灣電子治理願景工作坊全體會議決選結果

議題一

項目	願景一	願景二	願景三 3
政府組 1	**G1.**由政府針對網路之管理與品質立法(EX：電信市場主導之問題)並調整至一般大眾能負擔之網路費用，或補助相關費用給偏遠地區，另結合企業、ＮＰＯ、各業界進行資訊教育推廣(EX：建立諮詢系 3	**G1.**結合地方、中央政府建立單一窗口(EX：政府網頁個人化)。訓練第一線人員或資安人員後續資料整合技術，並對其業務分類、分級(EX：對稅收稅率制定之政策)。	**G1.**要求跨部門協商，各部會首長定期開會以利資訊流通，當災難發生時，可即時獲取各單位之資訊。
	G2.由政府成立推動小組(可採發包、民營化、公開招標方式)並結合電信業者，制定相關行動上網裝置及資訊交換平台的標準。		**G2.**由政府輔導或委託政府組織成立各地服務中心，即時提供公共訊息。
			G3.公共服務資訊可透過交通工具系統、ＰＤＡ等媒介，由民眾自行訂閱想要的即時資訊。
業界組	**B1.**企業提供業界資訊平台分享，與政府平台進行部份整合 2	**B1.**提供政府資訊電子影像並普及化，讓政府電子平台能夠及時傳輸訊息及回覆。	**B1.**企業提供業界資訊平台分享，與政府平台進行部份整合。
	B2.政府可透過企業資源（非政府的館藏）進行合作達到資訊共享。		**B2.**政府可透過企業資源（非政府的館藏）進行合作達到資訊共享。
	B3.公共服務資訊的建立，應有競爭與監督機制，並採取使用者付費	2	**B3.**公共服務資訊的建立，應有競爭與監督機制，並採取使用者付費
NPO組	**N1.**由政府部門編列預算及做規劃，建置基礎網路設備，讓光纖能到每一戶家庭；並建置都市、戶外	**N1.**政府應成立高層級資訊主責單位，如:資訊部、資訊局、獨立預算、獨立人事編制，由其主責全國	**N1.**政府提供不同媒介的平台提供災難、治安、交通、老人安全的資訊、即時發布、傳遞與回報。 1

	無線網路環境，讓民眾能隨時隨地高速上網，獲取資訊，尤其離島、偏遠地區鄉鎮，更要完善整理。ＮＧＯ、ＮＰＯ也可透過向企業募款，發展爲區域性資訊提供中心，且與各縣市政府，在地教育訓練機構合作，提供教育訓練、規廣，鼓勵銀髮族及身心障礙者上網。	各資訊相關政策規劃、推行。(地方主管機關要配合) 1 **N2.**政府應透過立法或行政命令發佈，破除各部門、單位隔閡，加速達成資訊整合系統，提供便民服務。(如：戶政、地政、健保局、國稅局資訊整合)，讓民眾至任一公部門均可辦理相關業務，免於奔波。 3	

議題一

項目	願景一	願景二	願景三
	N2.公部門補助公民每人行動電話(如：ＰＤＡ)，作爲公民接受政府訊息、查詢資訊政府可規劃二手設備流通、交換平台、提供公部門、學校釋出舊設備(如：電腦)，並開放偏遠地區有需求單位(如：學校、ＮＧＯ、ＮＰＯ團體)申請，達到物盡其用且提供需求單位擁有充足資訊收發載具目的。 **N3.**以及回報資訊載具。達成雙向資訊回報、流通功能。		
公民組 1	**C1.**政府須建立友善的電信環境，成立網路費率審議委員會，制定費率的上限，並創造公平競爭的獎勵投資機制與誘因以提高網路服務的品質。	**C1.**配合軟硬體的行動方案建置 (1)公民可透過電視、手機代替電腦介面，以遙控器或手機按鈕即可辦理相關業務。	**C1.**同３－１－１的行動方案政府須設置相關資訊平台，並可由公民設定往後需要收到資訊的類型(如交通)，方式(如簡訊或ｅ－ｍａｉｌ等)。

	C2.宣傳方式是透過多元公民教育管道：(1)戲劇(大眾傳播) (2)里辦公室負責(大聲公、宣傳車)。 **C3.**爲減少數位落差情形，針對弱勢族。	(2)亦可透過里辦公室及便利商店使用介面。 2	

議題二

項目	願景一	願景二	願景三
政府組	**G1**.針對個人資料保護加快立法腳步，並成立推動小組，進行討論及歸納民意，何謂個人資料之定義，並且成立監察單位監督個人機密資料的使用，若有違法使用之行爲應予以重罰。	**G1.**個人資料(生物特徵)由個人自行決定是否提供政府建檔，並由個人主導去決定是否公開，但如影響到政策面之資料(如綜所稅、房屋稅、地價稅、就醫資料等)政府機關有權查詢並整合，但不可外洩。	**G1.**由中央單位成立管理中心進行生物資料安全法之保護法之研究及制定。 **G2.**政府應針對個人資料加密，並建置完善的資料認證通行碼系統，並充分規畫出完善的資料分級系統，專人專案式的負責系統安全控管。
業界組	**B1** 立法確認隱私權與公共利益及企業利益之區別，立法上應明確訂定出主管機關。 **B2.**政府善盡監督之職責，調查並揭露任意侵害	**B1.**企業可協助政府推廣資訊安全教育，在技術研發及產品設計中應將資安視爲重要之務，對於內部對企業員工進行相關資安訓練，避免顧客個資外露。	**B1.**完整規範個人資料流通並設置最新個人辨識身份晶片卡，企業也可依此辨別是否聘用該員。 **B2.**企業研發電子辨識系統及設備，使用權限完善

	濫用個資之廠商，維護市場公平交易。	**B2.**企業本身應加強後台的安全機制,在資料使用上的安全可做多段加密,使用時會告知相關人員，MIS 與資料使用者權限必須明確劃分,而對於濫用資料之員工,除法律相關規定的懲處之外，亦有公司內部相關程序做爲嚇阻。 **B3.**個人隱私權(透過立法規範)資料使用每一次均需付費（例如ＫＴＶ），部分給被使用人部分給資料處理廠商，若有侵權，受害人可得到補償。	分級，系統之軟硬體由政府出資協同研發，並監控研發之安全性措施。
NPO組	**N1.**立法爲首要條件，並建置專責單位，進行教育與宣傳，使民眾瞭解、知情，並強化/強制執行與打擊網路犯罪行爲。	**N1.**個人資訊依存取資訊的重要性分級(立法定義分及種類或業界訂定同一標準)，資訊被使用時，應即時通知當事人，並由個人決定是否允許。	**N1.**政府建置全民個人辨識資料庫，由戶政機關採集個人指紋、DNA，發展不可否認性之機制(如perfect ID、自然人憑證)，並建立分級制度使用之。
公民組	**C1**.根據願景內容，對現有個人資訊保護法做修正，因爲目前來說，民眾對於個人資訊保護法的內容不清楚、不了解。	**C1.**個人資料藉由數位化做認證，認證分層級(一般身分、個人資料、便民資料、個人財產資料)。	**C1**.個人資料的認證，必須有加密動作，透過手機等不同介面，加以讀取、辨識，個人有權決定是否提供個人資訊之使用，並提供教育作是前主動告知，家所有個資作成資料庫，提防、避免犯罪問題。

議題三 電子治理願景與方向：情境規劃的應用

項目	願景一	願景二	願景三
政府組	**G1.**政府成立電子政治平台實驗特區及系統，試行此超級政府系統，做爲"全國推行"之準備。(加強民眾參與)。	**G1.**公民記者制度目前已存在目前該執行的是賦予公權力及強制性，並要求政府官員應定期回應與執行。 2	**G1**.當電子治議發揮到極致時，人民可以隨時罷免政府領導人、官員，且所有公投議題均可透過網路、手機、PDA 投票表決。
	G2.由中央機關授與民間組織或企業搜集議會問政及政府政策資料將其全程透明化，並錄影記錄並培訓電子廉能志工，附予適當權力，進行監督。		
	G3.議會問政結合手機，視訊系統公開化，公民可即時檢驗及投票，並可同時參與進行提問及表達意見，相關部門也應有所回應及配套。 2		3
業界組	**B1.**限制立法者隱藏問政資訊的職權，不公開部分須經過公投表決同意。	**B1.**成立基金會：例如舉辦民意統計調查、論壇活動、提高民眾關注力藉可營造企業形象。	**B1.**民意機關之經費編列及支出（預算及決算）的寫法減少專業術語，內容須由公民代表審核監督通過。
		B2.該電子平台對企業而言可藉由該網路平台收集到一些企業想收集的資訊，一方面資訊可信度高，一方面節省資訊收集成本。	**B2**.企業可藉由聯盟方式，集各企業之技術，設計專屬公民執行政權之設備。例如:數位手錶。
		B3.公民記者平台應加入評等及審核機制。	**B3.**企業協助政府建立電子平台由政府付費，企業可研發相關設備如電腦、PDA 或特殊通訊器材，可線上連署及上網投票，達到公民直接民主的境界。

	B2.發展數位語音或手寫報馬仔平台，讓非電腦使用者也能輕鬆隨時使用。		
NPO 組	**N1.**開設頻道、MOD、數位資料庫，無須遷就時空之限制，提供中央議會、地方議會、公聽會等未剪輯之影音資料，提供民眾即時與事後針對議題或人物的蒐尋與觀看，以利落實對政府的監督。 **N2.**政府可與各有線、無線電視台合作，請電視台開設特定時段，供公部門、及各不同團體(如NGO、NPO)針對公共政策或議題做討論。	**N1.**賦予直接民主法規及行政命令位階，給予公務員辦理事務之權衡依據，得依意見反應程度及質量加以衡量。 **N2.**建置平台彙整意見並送交行政、立法部門 (1)由 NPO、NGO，一般個人設定討論議題 (2)通過設定門檻(如單一討論串超過 5000 篇討論量)可提案 (3)提案內容由專人(建議爲立場中立之NPO、NGO)彙整意見與建議，送交各級立法單位提案及相關行政單位參採。	**N1.**企業協助政府建立電子平台由政府付費，企業可研發相關設備如電腦、PDA 或特殊通訊器材，可線上連署及上網投票，達到公民直接民主的境界。 **N2.**提供安全之時間與場所，以及程式驗證、避免民眾在非自願的情況下進行投票，並留存紙本投票系統雙軌並行，提供民眾自由選擇。
公民組	**C1.**政府應立法並設置基金會(含政府官、事務官、學者、NPO、私人企業的代表)，建置包含：(1)政策	**C1.**連接議題三願景一第一點的行動方案，在分層的各項議	**C1.**針對電子投票的部分，採取分階段先開放的方式，首以不在籍的海外學子，接以本島外出就業

	執行所有記錄、(2)經費使用、(3)政治人物，選舉政策落實的分層資料庫，提供迅速、完整、便利、不同需求的服務，且須公開徵選來自民間也了解政府部門運作的專案管理人。(同版主概念)	題中，開設多場的守門人會議，供民眾線上討論。	者、就學學子跨域投票，並連結議題一願景二第一點方案，至便利商店、ATM投票。

附錄十二 2020 台灣電子治理願景工作坊議題願景名次表

項目	議題一			議題二			議題三		
	願景一	願景二	願景三	願景一	願景二	願景三	願景一	願景二	願景三
第一名	**G1**由政府針對網路之管理與品質立法(EX：電信市場主導之問題)並調整至一般大眾能負擔之網路費用，或補助相關費用給偏遠地區，另結合企業、ＮＰＯ、各業界進行資訊教育推廣(EX：建立諮詢系統)	**N1**政府應成立高層級資訊主責單位，如:資訊部、資訊局、獨立預算、獨立人事編制，由其主責全國各資訊相關政策規劃、推行。(地方主管機管要配合)	**N1** 政府提供不同媒介的平台提供災難、治安、交通、老人安全的資訊、即時發布、傳遞與回報。	**G1**.針對個人資料保護加快立法腳步，並成立推動小組，進行討論及歸納民意，何謂個人資料之定義，並且成立監察單位監督個人機密資料的使用，若有違法使用之行為應予以重罰。	**G1**.個人資料(生物特徵)由個人自行決定是否提供政府建檔，並由個人主導去決定是否公開，但如影響到政策面之資料(如綜所稅、房屋稅、地價稅、就醫資料等)政府機關有權查詢並整合，但不可外洩。	**G2**.政府應針對個人資料加密，並建置完善的資料認證通行碼系統，並充分規畫出完善的資料分級系統，專人專案式的負責系統安全控管。	**N1**.開設頻道、MOD、數位資料庫，無須遷就時空之限制，提供中央議會、地方議會、公聽會等未剪輯之影音資料，提供民眾即時與事後針對議題或人物的蒐尋與觀看，以利落實對政府的監督。	**N2**.建置平台彙整意見並送交行政、立法部門(1)由NPO、NGO，一般個人設定討論議題(2)通過設定門檻(如單一討論串超過5000 篇討論量)可提案(3)提案內容由專人(建議為立場中立之NPO、NGO)彙整意見與建議，送交各級立法單位提案及相關行政單位參採。	**C1**.針對電子投票的部分，採取分階段先開放的方式，首以不在籍的海外學子，接以本島外出就業者、就學學子跨域投票，並連結議題一願景二第一點方案，至便利商店、ATM 投票。

項目	議題一			議題二			議題三		
	願景一	願景二	願景三	願景一	願景二	願景三	願景一	願景二	願景三
第二名	**B1**企業提供業界資訊平台分享，與政府平台進行部份整合。	**C1**配合軟硬體的行動方案建置 (1)公民可透過電視、手機代替電腦介面，以遙控器或手機按鈕即可辦理相關業務。 (2)亦可透過里辦公室及便利商店使用介面。	**B3** 公共服務資訊的建立，應有競爭與監督機制，並採取使用者付費	**N1**.立法爲首要條件，並建置專責單位，進行教育與宣傳，使民眾瞭解、知情，並強化/強制執行與打擊網路犯罪行爲。	**N1**.個人資訊依存取資訊的重要性分級(立法定義分及種類或業界訂定同一標準)，資訊被使用時，應即時通知當事人，並由個人決定是否允許。	**N1**.政府建置全民個人辨識資料庫，由戶政機關採集個人指紋、DNA，發展不可否認性之機制(如perfectID、自然人憑證)，並建立分級制度使用之。	**G3.**議會問政結合手機，視訊系統公開化，公民可即時檢驗及投票，並可同時參與進行提問及表達意見，相關部門也應有所回應及配套措施。	**G1**.公民記者制度目前已存在目前該執行的是賦予公權力及強制性，並要求政府官員應定期回應與執行。	**N1**.企業協助政府建立電子平台由政府付費，企業可研發相關設備如電腦、PDA或特殊通訊器材，可線上連署及上網投票，達到公民直接民主的境界。

附錄

項目	議題一			議題二			議題三		
	願景一	願景二	願景三	願景一	願景二	願景三	願景一	願景二	願景三
第三名	**G1**由政府針對網路之管理與品質立法(EX：電信市場主導之問題)並調整至一般大眾能負擔之網路費用，或補助相關費用給偏遠地區,另結合企業、ＮＰＯ、各業界進行資訊教育推廣(EX：建立諮詢系統)	**N2**政府應透過立法或行政命令發佈，破除各部門、單位隔閡，加速達成資訊整合系統，提供便民服務。(如：戶政、地政、健保局、國稅局資訊整合)，讓民眾至任一公部門均可辦理相關業務，免於奔波。	**G2** 由政府輔導或委託政府組織成立各地服務中心，即時提供公共訊息。	**B2**.政府善盡監督之職責，調查並揭露任意侵害濫用個資之廠商，維護市場公平交易。	**C1.**個人資料藉由數位化做認證，認證分層級(一般身分、個人資料、便民資料、個人財產資料)。		**C1**.政府應立法並設置基金會(含政府官、事務官、學者、NPO、私人企業的代表)，建置包含：(1)政策執行所有記錄、(2)經費使用、(3)政治人物，選舉政策落實的分層資料庫，提供迅速、完整、便利、不同需求的服務，且須公開徵選來自民間也了解政府部門運作的專案管理人。(同版主概念)	**N1.**賦予直接民主法規及行政命令位階，給予公務員辦理事務之權衡依據，得依意見反應程度及質量加以衡量。	**B1.**民意機關之經費編列及支出（預算及決算）的寫法減少專業術語，內容須由公民代表審核監督通過。

附錄十三 2020 台灣電子治理願景工作坊行動方案產出

議題一

願景一

1.企業可藉由社會風氣責任的帶動，來回饋及彌補數位落差

2.企業可提供多樣性的付費服務，以網路資通整合減少落差。

3.加強企業資訊部門的強度與獨立性，而非只將其作爲單純的電腦維修。該部門應有研發系統的能力，然而操作系統的成員需與研發成員區隔以避免舞弊。開發簡易操作軟體以減少數位落差。

願景二

1. 提供政府資訊電子影像並普及化，讓政府電子平台能夠及時傳輸訊息及回覆。

願景三

1.企業提供業界資訊平台分享，與政府平台進行部份整合。

2.政府可透過企業資源（非政府的館藏）進行合作達到資訊共享。

3.公共服務資訊的建立，應有競爭與監督機制，並採取使用者付費。

議題二

(一)

1.立法確認隱私權與公共利益及企業利益之區別，立法上應明確訂定出主管機關。

2.政府善盡監督之職責，調查並揭露任意侵害濫用個資之廠商，維護市場公平交易。

(二)

1.企業可協助政府推廣資訊安全教育，在技術研發及產品設計中應將資安視爲重要之務，對於內部對企業員工進行相關資安訓練，避免顧客個資外露。

2.企業本身應加強後台的安全機制,在資料使用上的安全可做多段加密,使用時會告知相關人員，MIS 與資料使用者權限必須明確劃分,而對於濫用資料之員工,除法律相關規定的懲處之外，亦有公司內部相關程序做爲嚇阻

3.個人隱私權(透過立法規範)資料使用每一次均需付費（例如ＫＴＶ），部分給被使用人部分給資料處理廠商，若有侵權，受害人可得到補償。

(三)

1.完整規範個人資料流通並設置最新個人辨識身份晶片卡，企業也可依此辨別是否聘用該員。

2.企業研發電子辨識系統及設備，使用權限完善分級，系統之軟硬體由政府出資協同研發，並監控研發之安全性措施。

議題三

(一)

1.發展數位語音或手寫報馬仔平台，讓非電腦使用者也能輕鬆隨時使用

2.限制立法者隱藏問政資訊的職權，不公開部分須經過公投表決同意

(二)

1.成立基金會：例如舉辦民意統計調查、論壇活動、提高民眾關注力藉可營造企業形象

2.該電子平台對企業而言可藉由該網路平台收集到一些企業想收集的資訊，一方面資訊可信度高，一方面節省資訊收集成本。

3.公民記者平台應加入評等及審核機制

(三)

1.民意機關之經費編列及支出（預算及決算）的寫法減少專業術語，內容須由公民代表審核監督通過。

2.企業可藉由聯盟方式，集各企業之技術，設計專屬公民執行政權之設備。例如:數位手錶

3.企業協助政府建立電子平台由政府付費，企業可研發相關設備如電腦、PDA 或特殊通訊器材，可線上連署及上網投票，達到公民直接民主的境界。

附錄十四 2020 台灣電子治理願景工作坊活動實錄

2020台灣電子治理
願景工作坊

2020台灣電子治理 願景工作坊
淡江大學公共行政學系
專家 NPO
平台

2020台灣電子治理 願景工作坊
主辦單位 行政院研究發展考核委員會
協辦單位
政治大學公共行政學系
世新大學行政管理學系
淡江大學公共行政學

附錄十五 2020 台灣電子治理願景工作坊前後測問卷

A1. 請問您從哪裡知道有關這次願景工作坊的消息？

□(1) 宣傳海報及宣傳單　□(2) 親朋好友告知　□(3) 學校通知
□(4) 網路或電子郵件　□(5) 主辦單位邀請　□(8) 其他 _____（請說明）

A2. 請問您爲什麼參加這次願景工作坊？

□(1) 對於電子治理的議題有興趣
□(2) 希望能影響電子治理的決策
□(3) 盡台灣公民之義務
□(4) 主辦單位邀請
□(5) 想賺點錢　□(6) 因爲議題跟自己的權益有關
□(7) 長官指派　□(8) 其他 _____

◎接下來，我們想要請教您一些與電子治理相關的問題

B1. 請問以下何者爲發展台灣電子化政府的主要負責單位？

□(1)行政院文化建設委員會　□(2)行政院研究發展考核委員會
□(3)行政院國家通訊傳播委員會　□(4)行政院國家科學委員會
□(5)行政院經濟建設委員會

B2. 請問台灣第一階段的電子化政府計畫開始於何時？

□(1)民國70年　□(2)民國75年　□(3)民國80年　□(4)民國87年
□(5)民國90年

B3. 請問臺灣的電子化政府發展迄今共分爲幾個階段?

□(1)一個　□(2)兩個　□(3)三個　□(4)四個　□(5)五個

B4. 請問強調「主動服務，服務到家」是台灣電子化政府哪一階段的目標？

□(1)第一階段　□(2) 第二階段　□(3) 第三階段　□(4) 第四階段

□(5) 第五階段

◎再來我們想請教您一些與審議式民主相關的問題

C1. 請問下列何者爲審議式民主的進行模式?

□(1) 政策德菲法 □(2) 腦力激盪法 □(3) 多元流程模式

□(4) 願景工作坊 □(5) 漸進主義模式

C2. 請問一般來說，願景工作坊的參與人數爲何?

□(1) 五到十人 □(2) 十一人到十五人 □(3) 十六人到二十人

□(4) 二十一到二十五人 □(5) 二十六人到三十人

C3. 請問下列何者不可爲願景工作坊的參與者?

□(1) 政府官員 □(2) 非營利組織 □(3) 一般民眾 □(4) 企業人士

□(5) 以上皆可

C4. 請問審議式民主最重要的目的爲何?

□(1) 讓專家可做出決策 □(2) 凝聚共識並做出決策

□(3)給公民一個抒發己見的機會 □(4) 使政府能迅速決定政策

□(5) 讓企業能掌握政策走向

◎下面是一些有關您平常參與公共事務情形的問題，請依據您個人狀況勾選一個適當的答案

D1. 請問您平時從哪裡得到有關國家大事的消息主要資訊來源爲何？

□(1) 電視媒體 □(2) 報紙 □(3) 雜誌 □(4) 宣傳海報

□(5) 親朋好友告知 □(6) 師長的告知 □(7) 網路資訊

□(8) 電子郵件 □(9) 廣播 □(10)其他_____

D2. 請問您曾經在立法委員選舉時投票嗎？

□(1) 從來不會 □(2) 偶爾 □(3) 經常 □(4) 每次都參加 □(5) 不知道

D3. 請問您曾經在縣市長選舉時投票嗎？

□(1) 從來不會 □(2) 偶爾 □(3) 經常 □(4) 每次都參加 □(5) 不知道

D4. 請問您平時會和其他人討論國家大事嗎？

□(1) 從來不會 □(2) 偶爾 □(3) 經常 □(4) 不知道

D5. 請問您是否曾經主動向民意代表陳情或表達意見？

□(1) 從來沒有 □(2) 一次 □(3) 二到四次 □(4) 五次以上

D6. 請問您是否曾經主動向政府部門陳情或表達意見？

□(1) 從來沒有 □(2) 一次 □(3) 二到四次 □(4) 五次以上

◎接下來要請教的是您對於公共事務的態度

E1. 有人說「政府官員很關心一般人的想法」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

E2. 有人說「民意代表很關心一般人的想法」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

E3. 有人說「政治太複雜了，一般人是無法了解的」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

E4. 有人說「公民參與僅具有象徵意義，民眾的意見在政策過程中並無法產生實質作用」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

E5. 有人說「專業性的政策事務，還是應交由專家學者來決定」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

E6. 有人說「民眾通常無法瞭解政府各項政策事務中所涉及的專業性」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

E7. 有人說「相對於民眾，公務人員較能依照專業進行決策與判斷」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

E8. 有人說「民眾所提出的政策建議大多不具實質意義」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

E9. 有人說「一般人對政府的政策沒什麼影響力」，您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對

□(4) 反對　　□(5) 非常反對　□(6) 無意見/不知道

E10. 您認爲您自己的意見值得政府參考嗎？

□(1) 非常值得　　□(2) 值得　　□(3) 普通　□(4) 不值得
□(5) 一點也不值得　□(6) 無意見

E11. 有人說「即使別人不同意我的意見，我也應該勇敢的講出來」，請問您同意這種說法嗎？

□(1) 非常同意　□(2) 同意　　□(3) 不同意也不反對
□(4) 反對　　□(5) 非常反對　□(6) 無意見/不知道

E12.整體而言，您相不相信我們的中央政府？

□(1) 非常相信　　□(2) 相信　　□(3) 普通 □(4) 不相信
□(5) 非常不相信　□(6) 無意見/不知道

E13.整體而言，您相不相信我們的_____（依據受訪者住所）縣（市）政府？

□(1) 非常相信　　□(2) 相信　　□(3) 普通 □(4) 不相信
□(5) 非常不相信　□(6) 無意見/不知道

◎接下來請教您有關個人網路使用情形

F1. 請問您平均一天(非上班時間)花多少時間上網？

□(1) 不到半小時　　□(2) 半小時以上，不到1小時
□(3) 1小時以上，不到3小時　　□(4) 3小時以上，不到5小時
□(5) 5小時以上，不到10小時　　□(6) 10小時以上

F2. 請問您曾使用個人手機、PDA 瀏覽網頁、或收e-mail 嗎？(複選)

□(1) 個人手機　　□(2) PDA
□(3) 沒有使用

F3. 請問您曾在網路上從事休閒活動（線上遊戲、收聽線上音樂、電影等）嗎？
□(1)有　　□(2)沒有

F4. 請問您曾在網路上使用線上傳呼軟體（MSN、ICQ、Yahoo 即時通等）和您的親人好友聯絡嗎？
□(1)有　　□(2)沒有

F5. 請問您曾在網路上搜尋生活資訊（如氣象、車票等）嗎？
□(1)有　　□(2)沒有

F6. 請問您曾經透過網路處理個人金融（網路銀行存匯、轉帳、繳費、股票買賣等）嗎？
□(1)有　　□(2)沒有

F7. 請問您曾在網路上查詢產品資訊或比價嗎？
□(1)有　　□(2)沒有

F8. 請問您曾在網路上販售或購買商品嗎？
□(1) 買方　□(2)賣方　□(3) 兩者皆有　□(4) 皆沒有

◎個人基本資料

G1. 出生年月：民國 ____ 年 ____ 月

G2. 最高學歷：□(1) 小學(肄業)畢業或以下　□(2) 國中或初中(肄業)畢業
□(3) 高中職(肄業)畢業　□(4) 專科
□(5) 大學(肄業)畢業　□(6) 研究所(肄業)以上

□(7) 其他

G3. 請問您現在的主要職業是什麼？

□(1)軍公教人員 □(2)民營公司員工 □(3)公司、商店或執業場所負責人

□(4)領有專業證照的自由業(如醫師、會計師、建築師、律師等)

□(5)參加職業工會的工人 □(6)農漁民 □(7)學生

□(8)家庭主婦 □(9)無業 □(10)退休人員

□(11) 其他：_____

G4. 目前居住地：_____縣(市)_____鄉鎮(區)

G5. 性別：□(1)男 □(2)女

附錄

感謝您兩天來對於「**2020 台灣電子治理願景工作坊**」的認真投入與參與，為了進行更深入的研究，我們準備以下問卷，希望能瞭解您參與的狀況，以及對於此次 2020 台灣電子治理願景工作坊的看法。問卷編號僅為對照前後測資料，您的答案***僅作為學術研究之用***，個人相關基本資料***不會公開及外洩***，煩請您據實填答，使本研究能順利完成。謝謝！！

電子治理研究中心

計畫主持人：政治大學公共行政學系 陳敦源副教授

協同主持人：世新大學行政管理學系 胡龍騰助理教授

淡江大學公共行政學系 曾冠球助理教授

敬上

◎首先我們想要請教您一些關於本次願景工作坊會前預備的問題

A1. 對於本次大會所準備的參考資料，在參加會議前您閱讀得如何？

□(1) 全部閱讀　□(2) 大部份閱讀

□(3) 少部分閱讀　□(4) 無閱讀

A2. 對於本次大會所準備的四份劇本，在參加會議前您閱讀的如何？

□(1) 全部閱讀　□(2) 大部份閱讀

□(3) 少部分閱讀　□(4) 無閱讀

A3. 請問您認為本次會議所準備的資料難易度如何？

□(1) 完全看不懂　□(2) 只看的懂一小部分　□(3) 普通

□(4) 大部分可以看懂　□(5) 全部看懂　□(6) 無意見/不知道

A4. 請問本次會議所提供的參考資料，讓您對瞭解電子治理願景的議題是否有所幫助？

□(1) 完全沒幫助　□(2) 不太有幫助　□(3) 普通

□(4) 有點幫助　　□(5) 非常有幫助　　□(6) 無意見/不知道

A5. 請問本次會議所提供的『劇本』，讓您在思考台灣的電子治理願景上，是否有幫助？

□(1) 完全沒幫助　　□(2) 不太有幫助　　□(3) 普通
□(4) 有點幫助　　□(5) 非常有幫助　　□(6) 無意見/不知道

◎接下來我們想要請教您一些關於參與本次願景工作坊的問題

A6. 請問專家演講對您瞭解什麼是『願景工作坊』，是否有所幫助？

□(1) 完全沒幫助　　□(2) 不太有幫助　　□(3) 普通
□(4) 有點幫助　　□(5) 非常有幫助　　□(6) 無意見/不知道

A7. 請問專家演講對您瞭解電子治理的問題，是否有幫助？

□(1) 完全沒幫助　　□(2) 不太有幫助　　□(3) 普通
□(4) 有點幫助　　□(5) 非常有幫助　　□(6) 無意見/不知道

A8. 請問您在第一天的小組討論中常發言嗎？

□(1) 從未發言　　□(2) 不太發言　　□(3) 普通
□(4) 偶爾發言　　□(5) 經常發言　　□(6) 無意見/不知道

A9. 請問您覺得在第一天的小組討論時，每個人是否都有充分發言的機會？

□(1) 無發言機會　　□(2) 不太有機會　　□(3) 普通
□(4) 還算有機會發言　　□(5) 經常有機會發言　　□(6) 無意見/不知道

A10. 請問您在第二天的小組討論中常發言嗎？

□(1) 無發言機會　　□(2) 不太有機會　　□(3) 普通
□(4) 還算有機會發言　　□(5) 經常有機會發言　　□(6) 無意見/不知道

A11. 請問您覺得在第二天的小組討論時，每個人是否都有充分發言的機會？

□(1) 無發言機會　□(2) 不太有機會　□(3) 普通
□(4) 還算有機會發言　□(5) 經常有機會發言　□(6) 無意見/不知道

A12. 請問您認爲在所有參與者一起參加的『全體會議』中，有關電子治理願景的行動方案是否有受到充分的討論？
□(1) 非常充分　□(2) 還算充分　□(3) 普通
□(4) 不太充分　□(5) 非常不充分　□(6) 無意見/不知道

A13. 整體說來，您在整個會議的過程是否有充分的機會提出您的想法和主張？
□(1) 非常充分　□(2) 還算充分　□(3) 普通
□(4) 不太充分　□(5) 非常不充分　□(6) 無意見/不知道

A14. 請問在整個會議過程中時，主持人是否鼓勵每個人都能表達意見？
□(1) 非常鼓勵　□(2) 還算鼓勵　□(3) 普通
□(4) 不太鼓勵　□(5) 非常不鼓勵　□(6) 無意見/不知道

A15. 整個會議過程，對於各種意見和看法，主持人是否維持中立的立場？
□(1) 非常中立　□(2) 還算中立　□(3) 普通
□(4) 不太中立　□(5) 非常不中立　□(6) 無意見/不知道

A16. 請問您對第一天所參加的那個小組所提出的願景是否感到滿意？
□(1) 非常滿意　□(2) 還算滿意　□(3) 普通
□(4) 不太滿意　□(5) 非常不滿意　□(6) 無意見/不知道

A17. 請問您對第二天所參加的『角色分組』小組所提出的行動方案是否感到滿意？
□(1) 非常滿意　□(2) 還算滿意　□(3) 普通
□(4) 不太滿意　□(5) 非常不滿意　□(6) 無意見/不知道

◎再來我們想要請教您一些關於參與本次願景工作坊之後的感想與問題

A18. 請問您對這次願景工作坊的目標瞭解嗎？

□(1) 非常瞭解　□(2) 還算瞭解　□(3) 普通
□(4) 不太瞭解　□(5) 非常不瞭解　□(6) 無意見/不知道

A19. 您認爲本次願景工作坊有達到目標嗎？

□(1) 完全達到目標　□(2) 達成大部分目標　□(3) 普通
□(4) 大部分未達成目標　□(5) 完全沒有達到目標　□(6) 無意見/不知道

A20. 請問您認爲本次願景工作坊所達成的結論是否具有可行性？

□(1) 非常具有可行性　□(2) 還算有可行性　□(3) 普通
□(4) 不太有可行性　□(5) 非常沒有可行性　□(6) 無意見/不知道

A21. 您認爲本次願景工作坊所達成的結論對於建構台灣電子治理願景是否具有重要性？

□(1) 非常重要　□(2) 還算重要　□(3) 普通
□(4) 不太重要　□(5) 非常不重要　□(6) 無意見/不知道

A22. 您是否同意『我希望這次會議所產生的結論，至少有一部份能成爲實際的政策行動』？

□(1) 完全同意　□(2) 還算同意　□(3) 普通
□(4) 不太同意　□(5) 完全不同意　□(6) 無意見/不知道

A23. 您是否同意『參與願景工作坊讓我聽到了許多過去沒聽過的想法』？

□(1) 完全同意　□(2) 還算同意　□(3) 普通
□(4) 不太同意　□(5) 完全不同意　□(6) 無意見/不知道

A24. 您是否同意『參與願景工作坊讓其他不同背景的人更有機會聽到我的意見』？

□(1) 完全同意　□(2) 還算同意　□(3) 普通
□(4) 不太同意　□(5) 完全不同意　□(6) 無意見/不知道

A25. 您是否同意『參與願景工作坊讓我更瞭解電子治理願景的問題』？

□(1) 完全同意　□(2) 還算同意　□(3) 普通
□(4) 不太同意　□(5) 完全不同意　□(6) 無意見/不知道

A26. 請問參加這次會議的經驗，是否會提高您參與公共事務的興趣？

□(1) 沒有提高　□(2) 只提高一些而已　□(3) 普通
□(4) 提高不少　□(5) 大幅提高　□(6) 無意見/不知道

A27. 請問您是否贊成未來政府在規劃電子治理政策時，舉辦類似的會議？

□(1) 非常贊成　□(2) 還算贊成　□(3) 普通
□(4) 不太贊成　□(5) 非常不贊成　□(6) 無意見/不知道

A28. 如果下次在邀請你參加類似的活動，您參加意願爲何？

□(1) 完全不會參加　□(2) 不太考慮參加　□(3) 普通
□(4) 會考慮參加　□(5) 一定會參加　□(6) 無意見/不知道

◎接下來我們想要請教您一些與電子治理相關的問題

B1. 請問以下何者爲發展台灣電子化政府的主要負責單位？

□(1) 行政院文化建設委員會　□(2) 行政院研究發展考核委員會
□(3) 行政院國家通訊傳播委員會　□(4) 行政院國家科學委員會
□(5) 行政院經濟建設委員會

B2. 請問台灣第一階段的電子化政府計畫開始於何時？

□(1) 民國70年　□(2) 民國75年　□(3) 民國80年　□(4) 民國87年
□(5) 民國90年

B3. 請問臺灣的電子化政府發展迄今共分爲幾個階段?

□(1) 一個 □(2) 兩個 □(3) 三個 □(4) 四個 □(5)五個

B4. 請問強調「主動服務，服務到家」是台灣電子化政府哪一階段的目標？
□(1)第一階段 □(2) 第二階段 □(3) 第三階段 □(4) 第四階段
□(5) 第五階段

◎再來我們想請教您一些與審議式民主相關的問題

C1.請問下列何者爲審議式民主的進行模式?
□(1) 政策德菲法 □(2) 腦力激盪法 □(3) 多元流程模式 □(4) 願景工作坊
□(5) 漸進主義模式

C2. 請問一般來說，願景工作坊的參與人數爲何?
□(1) 五到十人 □(2) 十一人到十五人 □(3) 十六人到二十人
□(4) 二十一到二十五人 □(5) 二十六人到三十人

C3. 請問下列何者不可爲願景工作坊的參與者?
□(1) 政府官員 □(2) 非營利組織 □(3) 一般民眾 □(4) 企業人士
□(5) 以上皆可

C4. 請問審議式民主最重要的目的爲何?
□(1) 讓專家可做出決策 □(2) 凝聚共識並做出決策
□(3) 給公民一個抒發己見的機會 □(4) 使政府能迅速決定政策
□(5) 讓企業能掌握政策走向

◎接下來要請教的是您對於公共事務的態度

D1. 有人說「政府官員很關心一般人的想法」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D2. 有人說「民意代表很關心一般人的想法」，請問您同意這種說法嗎？
□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D3. 有人說「政治太複雜了，一般人是無法了解的」，請問您同意這種說法嗎？
□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D4. 有人說「公民參與僅具有象徵意義，民眾的意見在政策過程中並無法產生實質作用」，請問您同意這種說法嗎？
□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D5. 有人說「專業性的政策事務，還是應交由專家學者來決定」，請問您同意這種說法嗎？
□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D6. 有人說「民眾通常無法瞭解政府各項政策事務中所涉及的專業性」，請問您同意這種說法嗎？
□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D7. 有人說「相對於民眾，公務人員較能依照專業進行決策與判斷」，請問您同意這種說法嗎？

□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D8. 有人說「民眾所提出的政策建議大多不具實質意義」，請問您同意這種說法嗎？
□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D9. 有人說「一般人對政府的政策沒什麼影響力」，您同意這種說法嗎？
□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D10. 您認爲您自己的意見值得政府參考嗎？
□(1) 非常值得 □(2) 值得 □(3) 普通 □(4) 不值得
□(5) 一點也不值得 □(6) 無意見

D11. 有人說「即使別人不同意我的意見，我也應該勇敢的講出來」，請問您同意這種說法嗎？
□(1) 非常同意 □(2) 同意 □(3) 不同意也不反對
□(4) 反對 □(5) 非常反對 □(6) 無意見/不知道

D12.整體而言，您相不相信我們的中央政府？
□(1) 非常相信 □(2) 相信 □(3) 普通 □(4) 不相信
□(5) 非常不相信 □(6) 無意見/不知道

D13.整體而言，您相不相信我們的_____（依據受訪者住所）縣（市）政府？
□(1) 非常相信 □(2) 相信 □(3) 普通 □(4) 不相信
□(5) 非常不相信 □(6) 無意見/不知道

◎個人基本資料

F1. 出生年月：民國　　年　　月

F2. 最高學歷：□(1) 小學(肄業)畢業或以下　□(2) 國中或初中(肄業)畢業
□(3) 高中職(肄業)畢業　□(4) 專科
□(5) 大學(肄業)畢業　□(6) 研究所(肄業)以上
□(7) 其他

F3. 請問您現在的主要職業是什麼？
□(1)軍公教人員　□(2)民營公司員工
□(3)公司、商店或執業場所負責人
□(4)領有專業證照的自由業(如醫師、會計師、建築師、律師等)
□(5)參加職業工會的工人　□(6)農漁民　□(7)學生
□(8)家庭主婦　□(9)無業　□(10)退休人員
□(11) 其他：_____

F4. 目前居住地：_____縣(市)_____鄉鎮(區)

F5. 性別：□(1)男　□(2)女

附錄十六 2020 台灣電子治理願景工作坊參與者名單暨訪談名單

政府組	姓名	服務單位	職稱
G1	廖靜芝	台中市政府	計畫處長
G2	蔡慶樺	屏東縣政府文化處	科員
G3	劉克章	經濟部知識資訊組	技士
G4	陳玫芬	台北市政府	資訊組組長
G5	周秀敏	行政院農委會林務局農林航空測量所	專員
G6	陳仕婕	行政院衛生署疾病管制局	科員
G7	林德芳	臺北市政府研考會	聘用企劃師
業界組	姓名	服務單位	職稱
B1	朱芬滿	台中市電腦商業同業公會	專案組經理
B2	丘廣嶺	建興電子	工程師
B3	衛敬文	太御科技企業股份有限公司	北區業務經理
B4	吳勝雄	台灣自來水公司	工程員
B5	黃英進	昂謙科技公司	經理
B6	竇尚志	瑞博資訊公司	副總經理
B7	張同鑫	康和資訊系統股份有限公司	系統分析師
B8	陳建良	長榮航太	副工程師
NPO 組	姓名	服務單位	職稱
N1	陳柏守	台灣青年公民論壇協會	常務理事
N2	翁正良	大同大學和平安全研究中心	研究助理
N3	張常昌	中山社區大學	幹事
N4	張柏年	台灣青年智庫學會	國際事務部副主任
N5	曾瀞萱	土城中正國中	教師
N6	顏子傑	國立臺灣大學 /臺北市澎湖縣同鄉會青年發展委員會	政治研究所

N7	李佩芳	財團法人台灣地理資訊中心	助理系統工程師
N8	黃健峰	公民監督國會聯盟	政策專員
N9	許美霞	自由業	
公民組	姓名	服務單位	職稱
C1	楊鎮宇	立穩營造	職工
C2	鄭佳文		
C3	周育貞		家管
C4	林宜蒓	自由業	補教老師
C5	賴進福	高雄市立興仁國中	幹事
C6	張仁偉	國立高雄應用科技大學	
C7	彭守均	待役	
C8	施怡寧	火鳳凰工作室	編劇
C9	陳美鳳	台北市政府文化局	副研究員
C10	孟繼汶		待業中
C11	李志文	ING 安泰	籌備主任
C12	林柏翰	巨豐業務單位	業務主任
C13	吳政倫	淡江大學	
C14	陳信守	政治大學東亞研究所	
C15	黃信維	私立元智大學	
如需要詳細的逐字稿內容請洽政治大學公共行政學系陳敦源教授 E-mail:donc@nccu.edu.tw			

附錄十七 2020 台灣電子治理願景工作坊會後深度訪談題綱

深度訪談大綱

1. 可不可以請您談一談爲什麼會想參加這個「2020 台灣電子治理願景工作坊」？在結束了這兩天的討論會議後，您覺得願景工作坊有沒有與您事前所預期的不同？爲什麼呢？

2. 請問您，關於我們所準備的議題手冊，在會議之前您有先看過嗎？不知道您看了多少？在您第一次看的時候，會不會不容易看懂？爲什麼？那您覺得這份資料內容的公正與客觀性方面怎麼樣？對您了解會議的主題有幫助嗎？那我們所準備的劇本呢？在您第一次看的時候會不會不容易看懂？爲什麼？

3. 在聽過專題演講：「台灣電子化治理相關政策與未來期許」、「電子治理與審議式民主之聯結」、「願景工作坊介紹」後，請問您覺得對您瞭解議題有無幫助？

4. 請問您對於第二天「角色扮演」這項活動的看法是什麼？您所被安排到的角色和您本身的價值觀（本來一向看重的觀念）有沒有不一樣？您覺得「角色扮演」對您去體驗複雜的2020 台灣電子治理問題有沒有幫助？爲什麼？

5. 請您談談在會議中和其他人一起討論時的感想，有沒有令您印象深刻的事情？過程中，您的意見有沒有產生改變？

6. 在小組討論的時候，您會不會經常想到 2020 台灣電子治理對我們一般民眾有什麼影響？您覺得其他人有沒有這樣想？在這種場合中，您是否能夠隨心所欲地發言？

7. 請問您在會議期間（9 月27 日及10 月18 日），是不是有跟會議以外的人分享您參加「2020 台灣電子治理願景工作坊」的感想？爲什麼？

8. 您滿意這份報告嗎？您認爲在這份報告中，是否有納入您的意見？您覺得這份報告是大家的共識嗎？在大家一起參加討論的情況下，爲什麼能夠出現共識？這是怎麼做到的？還是只反映少數人的意見？如果是這樣？應該怎麼

樣去改善？

9. 經過這次會議之後，您對「2020 台灣電子治理相關議題」的哪些觀點和態度有哪些轉變？爲什麼？

10. 請您談談您對於「2020 台灣電子治理願景工作坊」的整體的評價怎麼樣？(例如：小組成員在會議討論的表現？會不會影響政府的政策？增加您對於跟台灣電子治理有關的議題的了解？)

2020 台灣電子治理願景工作坊 深度訪談
深度訪談大綱（政府機關加強版）

1. 目前政府機關有類似的公民參與機制（如公聽會、說明會或網路論壇），實際運作的狀況如何？您的相關經驗又有哪些？您覺得願景工作坊和以上的公民參與方式有那些不同？

2. 在電子治理相關政策的規劃上，過去都是由行政部門和專業的人士來做決定，這次舉辦願景工作坊會不會和過去的決策方式有所衝突？會不會侵犯政府機關或長官的決策權？

3. 針對這次願景工作坊參與的公民、企業，及 NPO 代表，您覺得他們參與討論的能力如何？是不是都可以講出他們的道理？他們是比較站在私人的角度還是國家社會的角度來談問題？由他們來討論和由政府官員或學者討論有什麼不同？

4. 麻煩您舉出這次結論幾個比較具體的政策意見，您覺得這些意見有沒有說服力？他們的行政可行性如何？政治可行性如何？有沒有和政府部門既定政策方向或長官的意見不一樣的結論？在願景工作坊後，您覺得政府應如何處理會議結論(追問一致與不一致的處理方式)？這些結論對政策有沒有影響？(追問沒有影響狀況下的原因)從哪些地方可以看得出來？

5. 整體而言，這次舉辦願景工作坊對政府機關或社會的效用在哪裡（可追問教育、政策合法性、爭議的解決、決策的品質等）？有無負面的影響？您覺得您所服務的機關，未來是否可能採用願景工作坊(或類似的審議式民主模式)來處理公共事務的議題？

附錄十八 2020 台灣電子治理願景工作坊議題手冊

壹、前言

願景工作坊是一種具有審議民主精神的公民參與模式；透過願景工作坊的舉辦，參與者可對於所關懷的事務或議題，共同描繪未來發展的願景與藍圖。

在工作坊的實際運作過程中，參與者將根據他們的經驗與期盼，檢視這些願景。願景工作坊強調收集參與者對於討論議題的看法與認知，以及與會者對於未來發展的態度與他們關切的項目。經過批判、提出觀點與思考願景的過程，提出他們的看法以及具體可行的行動方案。

本次願景工作坊的討論主題爲台灣2020電子治理未來願景的規劃，不同於以往的公民參與模式，台灣2020電子治理願景工作坊將突破「由上而下」或「由下而上」的單線運作模式，而以類似於網絡參與的方式擴大參與基礎。規劃中參與會議的人員將包含中央與地方層級之政府官員、業界、非營利組織及一般民眾。期望透過此一願景工作坊之舉辦，能使不同利害關係人對於電子治理未來願景，能夠相互對話、相互理解，進而型塑彼此之共同願景。

本次工作坊最主要的三個討論議題如下：

(一) 2020年民眾最希望政府電子治理所提供的服務內容是什麼？要如何作才能達到這樣的願景？

(二) 2020年政府電子治理推動過程中要如何平衡資訊公開與個人隱私的衝突？要如何作才能達到這樣的願景？

(三) 2020年台灣民主政治的發展，您會希望會因爲電子治理的進展而到什麼樣的程度？要如何作才能達到這樣的願景？

一、活動目的

公共討論可以進一步將公民參與的意見加入政府的計畫之中，並透過實際深度的討論與對話，強化公民對台灣未來電子化治理願景規劃的想像。在此活動結束後，預期可達到以下效益：

(一) 推廣並強化台灣民眾公民參與的精神，鼓勵公民能勇與表達自身意見，促進政府和民間的互動與合作。

(二) 凝聚台灣全體公民對於電子化治理的共識，可使全體社會不同的利益和價值考量能達到一個均衡點，在此基礎下所進行的各項決策會更具正當性。

(三) 透過公民參與的過程，一方面可以提升社會大眾應有之權益，另一方面更能讓民眾重視身爲台灣公民所應有的責任與義務。

(四) 多元意見可以獲得融合，不光是政府單方面的主

導政策，公民意見也能透過此次願景工作坊得以發聲，不同觀點的相互激盪和審慎思辯後的結論，才是真正足以作爲台灣 2020 年電子化治理的指導方針。

本活動能使政府和公民能一起提出相容的願景，並創造出屬於台灣自己的電子化治理方向，由政府逐步實現之，讓台灣能以電子治理的成果，站上國際舞台與世界接軌，並增加我國的國際競爭力。

二、執行團隊

計畫主持人	陳敦源	電子治理研究中心研究員 政治大學公共行政學系副教授
協同主持人	胡龍騰	電子治理研究中心研究員 世新大學行政管理學系助理教授
協同主持人	曾冠球	電子治理研究中心研究員 淡江大學公共行政學系助理教授
執行委員	李國田	行政院研究發展考核委員會 資訊管理處高級分析師
執行委員	林劍秋	財團法人資訊工業策進會 顧問規劃師
執行委員	朱斌妤	電子治理研究中心主任 政治大學公共行政學系教授
執行委員	黃東益	電子治理研究中心研究員 政治大學公共行政學系副教授
執行助理	呂季蓉	政治大學公共行政學系碩士
執行助理	梁芳瑜	淡江大學公共行政學系碩士生
執行助理	陳序廷	政治大學公共行政學系碩士生
執行助理	黃重豪	政治大學公共行政學系碩士生

執行助理	李基嘉	世新大學行政管理學系碩士生
執行助理	黃榮志	世新大學行政管理學系碩士生

三、活動議程

9 月 27 日（六）正式會議第一天	
時間	議程
09:00-09:30	報到
09:30-09:50	**開幕式**
09:50-10:30	**專題演講一** 台灣電子化治理相關政策與未來期許 發表人－宋餘俠 行政院研究發展考核委員會副主任委員
10:30-10:45	茶敘時間
10:45-11:00	**自我介紹**
11:00-11:40	**專題演講二** 電子治理與審議式民主之聯結 發表人－陳敦源 電子治理研究中心研究員 政治大學公共行政學系副教授
11:40-12:20	**專題演講三** 願景工作坊介紹 發表人－林子倫 台灣大學政治系助理教授
12:20-13:00	午餐時間
13:00-13:30	**分組會議**－ 閱讀可閱讀資料與劇本
13:30-14:30	**分組會議**－ 我們的主張（初步願景）
14:30-16:00	**分組會議**－ 我們的願景
16:00-16:30	茶敘時間
16:30-17:10	**全體會議**－ 報告各組願景
17:10-18:30	**全體會議**－ 比較、釐清與回應
18:30	晚餐時間

9 月 28 日（日）正式會議第二天	
時間	議程
08:30-09:00	報到
09:00-09:30	**全體會議** 會議進行方式說明與角色分組
09:30-09:45	茶敘時間
09:45-12:00	**分組會議** 好點子初選
12:10-13:00	午餐時間
13:00-13:30	**全體會議** 好點子說明
13:30-14:30	**全體會議**

	好點子決選
14:30-15:30	**全體會議** 好點子亮相
15:30-15:45	茶敘時間
15:45-17:00	**全體會議** 好點子上路，未來會更好
17:00	**閉幕式**

貳、願景工作坊介紹

願景，是策略管理的核心；願景亦是一種未來取向的前端價值觀。

願景工作坊最廣為人知的典範是丹麥的科技委員會，其在都市的生態維護與居住型態，以及未來的圖書館規劃等計畫中，納入「願景工作坊」的單元，以便引發民眾提出他們對於公共圖書中資訊科技的應用的觀點與看法。自此，願景工作坊也「外銷」到了歐盟，希望藉著願景工作坊來聯繫研究活動與社會的需求，而建立起一套廣泛的網絡。

檢視願景工作坊，可以發現其操作的最重要骨幹－「劇本」(scenario)，即是源自策略上一種「沙盤推演」的實踐，而策略的本身，又是軍事上計畫的一種藝術，這樣環環相扣的概念，皆指涉了願景工作坊在理論未來與實際上，可能提供的一種相關連結的建構、或是產生一個可模擬並且修正的具體參考指標。因此有必要透過願景工作坊這樣的實際運作，在產、官、民三方的參與之下，共同建構台灣在 2020 年電子治理的規劃景象。

一、何謂願景工作坊

近年來審議式民主（deliberative democracy，或譯為商議民主）熱潮席捲全球，此波審議式民主的發展，促進了公民的角色的積極參與，並且置入各個面向的利害關係人於其中，來模擬實踐、討論相關的政策議題。其中，願景工作坊（scenario workshop）是一種特別的會議形式，在工作坊進行期間，應有充分的時間進行腦力激盪、討論、表達與投票。工作坊的形式與基本規則都是確保讓參與者能言其所言，所有的想法都能被加以討論，以及建立一個行動計畫。換句話說，願景工作坊即是審議式民主理論中，一種植基於「未來」概念上的公民會議，依循批判、提出觀點與思考願景的過程，但更著重於提出特定地區未來可能發展的基本目標，而這些對於未來的期

待，則會在願景工作坊中進一步的被討論著。

二、願景工作坊的組成元素

願景工作坊最重要的核心除了透過劇本（scenario）將主題限定與問題聚焦後作爲發展願景起點的功能外，支撐整個願景工作坊組成運作，尚需下列因素的環環相扣的結合：

面向：界定問題領域，將問題所涉的不同層次展現出來，確定所提出的問題必須具體。

劇本：由主辦單位撰寫腳本，設定時空環境與特別事件其中必須包含各種面向、問題以及提供的解決方法；這個劇本所提供的解決方法可能是同一軸線上的幾個解決方式，每個劇本不見得包含全部的解決方式，但必須對所有的主題（theme）有所處理。透過劇本，讓參與者身處其中演練，以發現問題徵點、提供可行動方案、解決問題。

願景：與會者，根據所提供的劇本作爲一個起點，演練磨合後，共同有一可達到的期望圖像。

參與者：願景工作坊的參與者大約在二十五人到三十人之間，邀請對象爲不同的社會部門，如民眾、政治人物與政府官員、科技專家以及發明家與企業代表等，透過分組與角色的設定扮演，使參與者根據他們的經驗，檢視這些願景，並且提出他們的看法與可行的行動計畫，而每一組皆要討論正向與負向劇本，並比較自己小組的願景結論與之有何不同。

三、願景工作坊的規範

工作坊觸及不同科技類型之間的評估與選擇，除了議題不應過於狹窄外，更重要的是，願景工作坊像是一個參與者的行動場域，他們有機會影響決定而不是扮演背書的角色；其所討論議題必須社會有關，並且有凝聚當地共識的必要性，而透過專家知識與民眾經驗的交流，將會產生社會學習的效果，產生新的知識，因此在參與的過程中，必須謹守下列共識：

前提：願景工作坊是一種特別的會議形式，依循以下的規範。在工作坊進行期間，應有充分的時間進行腦力激盪、討論、表達與投票。工作坊的形式與

基本規則都是確保讓參與者能言其所言，所有的想法都能被加以討論，以及建立一個行動計畫。

流程：一般來說，工作坊的進行需要兩天時間，並且經過三個階段：批判、提出看法與行動計畫的具體化。在批判階段中，民眾以他們的經驗、觀點與知識，對於未來的發展表達意見，無論是正面或負面。願景工作坊的重點並非在這些不同的意見中挑選、或挑選與會者偏好的看法或是評估何種論點較為可行，之所以進行批判，目的在**協助新知識與行動計畫的產生**。我們可以從其中挖掘出某人對於未來期待的觀點與要素，並且與其他人的看法相結合。

產出：工作坊進行中，以批判階段所產生的知識為基礎，與會者將在提出看法的階段，形成他們對於議題的一致觀點。在行動計畫具體化的階段中，主要工作在於提出可以讓共識實現的行動計畫，面對計畫可能遭遇的阻礙，必須釐清不可忽視，與會者必須將問題與行動方案排列優先順序，指出哪些工作是必須完成的。

四、願景工作坊進行步驟

願景工作坊是一種特別的會議形式，有一定的程序和規則。在工作坊進行之前，主辦單位會先準備「議題手冊」，淺顯易懂地介紹會議所要討論的政策議題，並撰寫一套「劇本」，描述不同的政策方案所可能帶來的後果，讓參與者透過對劇本的批評來發展共同願景。

於願景工作坊的正式會議該如何建構共同的願景？

主要分為幾個步驟：

形成初步願景

參與者依身份（一般民眾和其他屬性代表）分成四組，進行型塑願景的分組討論。在分組討論中，與會者先對會議主題交換意見，並將意見彙整為本組的初步願景。

比較初步願景與劇本的差異

初步願景形成後，接著便要比較劇本與初步願景的差異。與會者針對劇本進行討論，並且將劇本的批評討論與會議主題關連起來，思考本組的初步願景，有沒有什麼需要修改的地方？

形成小組願景

做完劇本和初步願景比較之後，開始就討論主題（和每個子題）作逐項討論。與會者針對每個主題（子題）提出補充或修正意見，並進行討論，以形成共同的主張。每一分組推派一名或多位代表，在全體會議中報告本組共同願景。

報告各組願景

四個分組的所有與會成員，進行全體會議。每個分組報告該組的願景。每組報告完後，由其他三組進行批評與討論，再由報告組回應。全體成員對於四組各自提出的願景的討論著重於：哪些願景比較具體可行？哪些願景較難施行？四組願景的共同主張爲何？最明顯的差異又在哪裡？

型塑共同的願景

願景工作坊如果進行兩天，在報告、批評、討論各組願景之後，即結束第一天的會議。執行團隊於第一天會後，將四組所提供的願景，加以彙整成共同願景。整理完成的共同願景，列印給每個與會者，作爲第二天討論行動方案的基礎。

而在願景工作坊的正式會議中又該如何提出行動方案？行動方案的提出，有幾個程序：

角色分組

不同身份的參與者混合編成數組（通常是四組），組別可以「行動者」來分類，每組討論這類行動者應該做什麼，才能達到前一天所提出的共同願景。

以「國家職訓願景工作坊」爲例。角色分組是以政府部門、企業、民間職訓機構和學校這四類「職訓提供者」來區分。分組會議將從第一天的共同願景出發，來討論：爲了實現國家職訓的願景，政府、企業、民間職訓機構和學校這四種職訓提供者，應該做什麼，才能達到「共同的願景」（每組只討論分配到的那一類的職訓提

供者該做什麼）。

初選行動方案

在分組討論時，先由每位參與者輪流發言，提出自己的行動主張，說明本組所討論的行動者該做什麼，才能達到願景。這一階段的意見交換，主要在聆聽與說服。意見交換完畢後，每人提出自己的行動主張，然後進行票選，選出本組最受支持的五個行動方案，向全體會議報告。

行動方案的選擇可以有彈性。每個願景工作坊都可設計合適的方式來選擇行動方案。國家職訓願景工作坊曾經使用「K.J.法」來選擇行動方案。這種方法的好處是方案選擇的過程包含「審議」的精神。K.J.法的進行步驟如下。每位參與者將三個行動主張（數個可以彈性規定），寫在三張卡片上（每張卡片寫一個主張），然後以 K.J. 法進行歸納。主持人隨機請某人出牌，唸出其主張，詢問有沒有相同或類似的主張。若有，則覆誦「跟牌」的人所寫的內容，有疑義者詢問參與者可不可以歸爲同一類。將每個經過歸類的每個牌組的行動主張，清楚地講述一遍，詢問參與者對字詞的使用是否同意。計算牌組的張數，選出前五名。有張數相同以致無法決定前五名者，則進行表決。投票方式（例如每人投幾票）由參與者決定。

決選行動方案

各組推派代表，在全體大會上報告該組選出的五個行動主張。全體成員與會者便對這些行動方案進行投票。參與者每人有五票，他可以將五票集中投給一個方案，也可以分散投給不同的方案，但不能投給自己所屬的組別提出的主張。投票完畢後，工作人員統計得票最高的五個行動主張。五大行動方案經票選產生後，由提出該方案的組別推派代表，向與會者進一步闡明該方案的內容和提出主張的理由，接著由與會者進行討論。討論重點在於：這些主張具體上該怎麼樣做？可能會遇到什麼障礙，這些障礙該怎麼樣來克服？它需要有怎麼樣的配套措施，才能夠讓這個政策的實現更完美？透過討論，凝聚共識，以形成實現願景的行動計畫。願景工作坊獲致的結論，包括共同的願景與行動方案，向政府相關單位提出報告並提供決策參考。

Day1 了解與批評

先由專家介紹議題現況與未來發

Day1 形成初步願景

依身分分成四組，各組相互討論交換

Day1 比較初步願景與劇本

與會者針對劇本進行討論，並將劇本

Day1 形成小組願景

與會者對每個子題提出補充或修正

Day1 報告各組願景

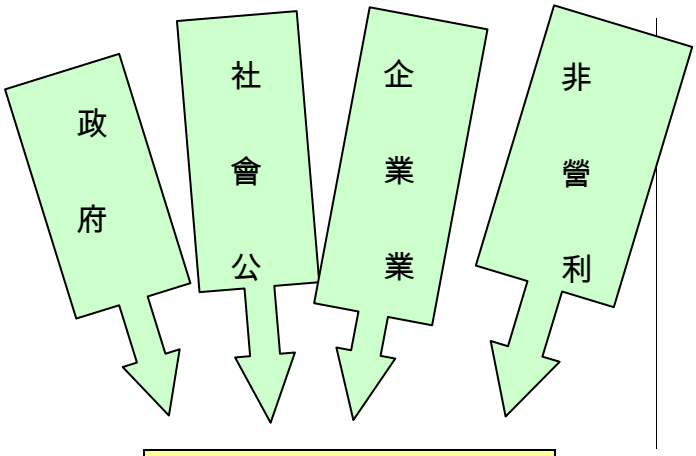
各組報告完後，由其他三組進行批評

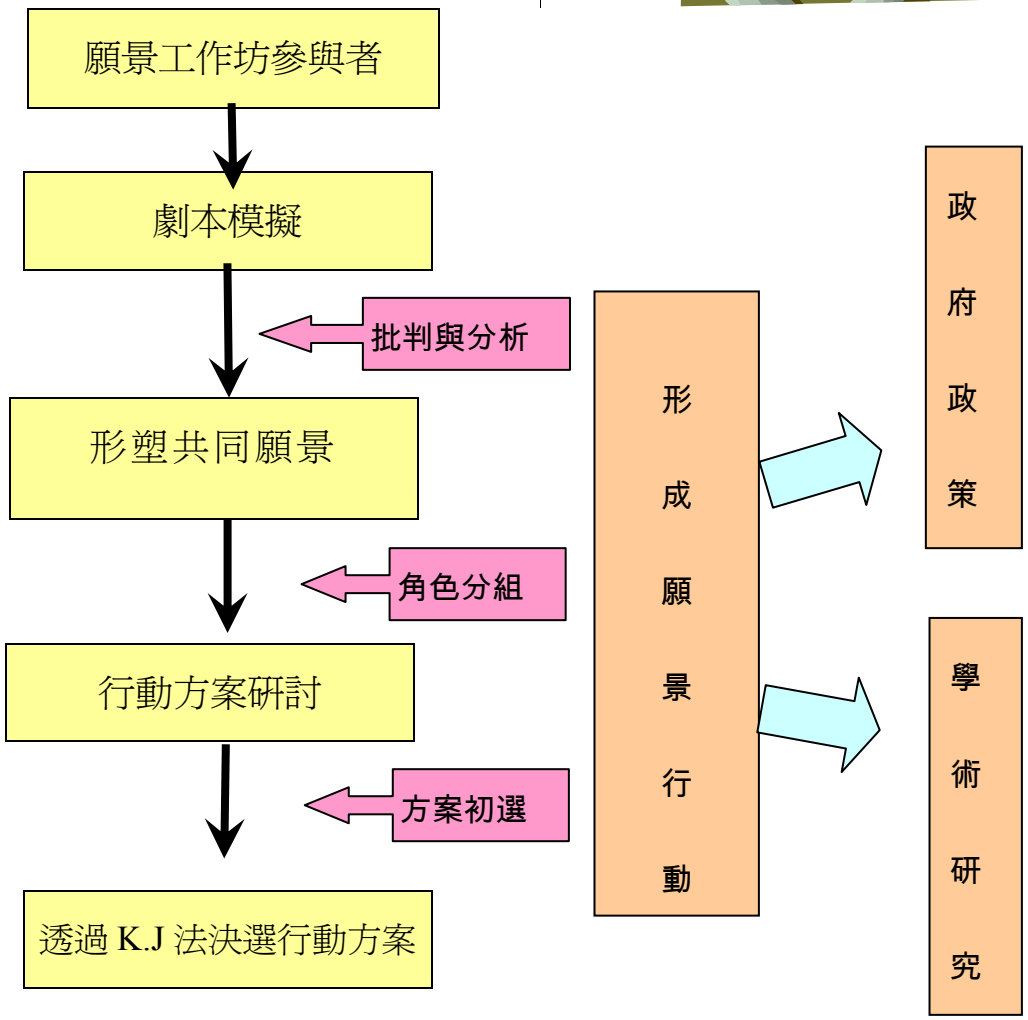
Day2 提出行動方案

不同身分者混合編組，各組進行初選

圖 1 願景工作坊進行流程圖

資料來源：本團隊自行整理


政府
社會公
企業業
非營利


願景工作坊參與者
劇本模擬
批判與分析
形塑共同願景
角色分組
行動方案研討
方案初選
透過 K.J 法決選行動方案
形成願景行動
政府政策
學術研究

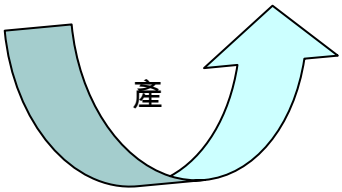


圖 2 願景工作坊架構示意圖

資料來源：本團隊自行整理

五、各國願景工作坊情形

如同公民陪審團與共識會議，願景工作坊也逐漸爲其他國家採用。就目前所知，至少有美國、英國、芬蘭、奧地利、義大利、法國、希臘、德國、西班牙、瑞典、葡萄牙、斯洛伐克等十二個國家舉辦過願景工作坊。這些工作坊，有不少是在歐洲覺醒願景工作坊（European Awareness Scenario Workshop, EASW）計畫下執行。EASW 是歐洲執委會第十三總署底下的計畫。它沿用並改進丹麥發展出來的願景工作坊，以探索可能的行動，促進歐洲各國社會環境的創新。它的主題原本著重在都市環境，近來逐漸擴展到和永續發展相關的層面上，例如衛生健康、運輸與資訊科技等。爲了在各國推展 EASW，歐洲執委會第十三總署委請義大利非營利組織 Foundation IDIS 設計與執行一套訓練課程，讓所有國家監督員都能在各國推動、規劃與執行 EASW。至於它的程序，我們將在底下適當的地方加以介紹。我們現在將援用前面對各國公民陪審團的比較模式來比較各國舉辦願景工作坊的經驗。各國願景工作坊舉辦次數概況如表 1，至於我國的案例則如表 2 所示。

表 1 各國願景工作坊舉辦次數

國家	次數
義大利	21
丹麥	5
西班牙	4

國家	次數
義大利	21
英國	3
奧地利	2
希臘	2
法國	1
斯洛伐克	1

資料來源：修改自林國明，行政民主之實踐，頁 60。

表 2 台灣的願景工作坊案例

活動名稱	舉辦時間
「醫療品質資訊公開」願景工作坊	2004.05.14、05.15
「國家職訓」願景工作坊	2004.12.10、12.11
「世新在大文山區的角色與定位」願景工作坊	2006.12.02、12.03
「二十一世紀台灣公民」願景工作坊	2007.07.14、07.15
「淡水河整治」願景工作坊	2007.11.25、11.26

活動名稱	舉辦時間
「中港大排規劃與使用」願景工作坊	2008.06.28、06.29

資料來源：本團隊自行整理

六、結論

自電子科技普遍化以來，人類食、衣、住、行，無一不朝與其更緊密結合的方向前進著，在此資訊科技的驅動下，或政府、或民間，藉著「資訊與通訊科技」（Information and Communication Technology, ICT），大幅的提升了決策與過程的效率與效能；我們的生活，已經與資訊科技密不可分。而 2020 年電子治理願景工作坊，乃是在台灣永續發展的基石上，整合電子資訊的發展，以一步一腳印的穩紮穩打姿態，擘行當下；以匯聚歷史的智慧經驗，綜視過去；以前驅者的先知灼見，聚焦前瞻；藉著工作坊所有參與者的共同努力，在討論問題與發展對策的雙軸線上，對未來的治理圖像作出建構，並且促進民眾在公共議題上的了解與參與。

參、何謂「電子治理」？

一、背景介紹：好萊塢電影對電子治理的想像

網路社會的治理問題，是影劇界想像未來的主要元素，許多美日電影漫畫卡通的主要題材所在，下面提供大家四部影片之簡介作爲引介電子治理的開場白。

（一）網路上身[1]（The Net） 1995

「網路上身」是一部以人類過度依賴電腦，以至於和周圍環境嚴重隔離的故事架構而發展出來的驚悚片。珊卓布拉克在片中飾演一個害羞內向的電腦程式分析師安琪拉，不和親戚朋友往來的她，是在家中工作的 SOHO 族，平常與外界的聯繫，完全憑靠個人電腦。一次工作完畢後，安琪拉在無意間下載了有關地下恐怖份子組織的磁碟片，裡面儲存了重要的致命資訊。毫不知情的安琪拉帶著磁片，前往墨西哥度假，在異國浪漫氣息濃厚的外地，和一名英俊的男子墜入情網，兩人在海上出遊的時候，這名神秘男子卻對安琪拉展開殺機。九死一生，逃回都市的安琪拉發現自己所有「存在」的資料和證明，都被另一個陌生女子冒名頂替了，唯一能證明她身份的心理醫生，也在和她

[1] 劇情介紹擷取自
http://movie.starblvd.net/cgi-bin/movie/euccns?/film/1995/Net/Net.html

會面之後被暗殺了。

處境危險而展開逃亡的安琪拉，因爲恐怖份子捏造了一個犯罪紀錄的身份，逼得她無處可逃。現在她必須運用自己的電腦長才，想出一套足以擊敗對方，而且重新奪回原來的生活和身份的致勝絕招…。

（二）LIVE 殺人網站[2]（Untraceable） 2008

好奇絕對不只殺死貓，在無邊網路的世界，窺探的刺激絕對讓你沒命。精明幹練的警探珍妮佛隸屬於 FBI 的網路犯罪調查科，這個新成立約七年的部門，24 小時全天候監視偵辦網路犯罪。每天夜裡，她和搭檔葛瑞芬唐不停的瀏覽網頁，監視著奧勒岡州波特蘭市一帶的網路金融詐欺及性犯罪案，接到線報的兩人開始調查起一個名爲"一起殺人.com"的恐怖網站。 一開始，站長將一隻貓咪黏在老鼠板上等死，並在網路上即時聯播，之後一件件變態離奇的虐殺不停在網站上播放，造成廣大迴響與好奇的窺探點閱，卻也教珍妮佛與葛瑞頭痛不已，這名站長不只嗜好怪異，更是個網路高手，使得整個網站的伺服器主機位置始終成謎，他不停的挑釁警方並且毫不客氣的點出自己所在的位置。接著，一名當地人被押至貓咪的屠宰場，隨著網站點閱人數的激增，一步步加速著受害人死亡的速度，讓他們再也無法把這個詭異的"一起殺人.com"網站當作玩笑。第一位被害人遇害後，這個變態殺人狂開始在網站

[2] 劇情介紹擷取自 http://movie.pchome.com.tw/dvd_info.php?dvd_no=401

上貼出預告，點出下個被害者的姓名與照片，爲了揪出兇手珍妮佛前往波特蘭，與警局探員艾瑞克霸斯合作，成立跨部會專案調查小組，但隨著越接近核心，眼前的網路世界似乎成了無止盡空間，也讓兇手鎖定了她和她的搭檔...在無邊的網路世界裡，珍妮佛與艾瑞克要如何這個變態殺手，又要如何阻止不停湧入的網友，以減緩被害人死亡的速度...一方面被盯上的珍妮佛與家人又要如何脫身？

（三）全民公敵[3]（Enemy of the State） 1998

威爾史密斯在片中是位家庭事業有成的律師，巧遇一位久未謀面的朋友，他狼狽地央求史密斯救他，並在倉惶中拿了史密斯的名片後，便行色匆匆地逃跑了。就在他橫越馬路時，意外地發生車禍，當場死亡。此時史密斯已陷入一個難以脫身的謀殺案中，卻渾然不覺，因爲車禍喪生的友人，早已神不知鬼不覺地，將一張記錄著一樁國會議員謀殺的磁碟片，放在史密斯的袋子裡。原來謀殺國會議員的主謀強沃特和他的屬下，當時爲了取回磁碟片，正追殺著史密斯的朋友，而他們在車禍現場找到了史密斯的名片後，開始尋線跟蹤史密斯，用高科技的衛星監視，企圖嚴密控制史密斯的行蹤，藉以奪回磁碟片銷毀謀殺的證據，並殺人滅口。

家庭、事業與生命受到極大威脅的史密斯，唯一的救兵是曾爲安全局探員、現在是地下情報販子的金哈克曼，史密斯可以脫離高科技的監控，並反制強

[3] 劇情介紹擷取自 http://emovie.ettoday.com/emovie/article/22-3187.htm

沃特嗎？

（四）攻殼機動隊[4]（Ghost in the Shell） 1995

故事的背景舞台設在近未來的日本，還以香港的街道作爲基礎，大約2030 年代前後，在一個網絡與科技發展得極發達的社會，所有的資訊與連繫都已經高度的網路化，是資訊爆炸的年代。不過國家和民族的分界並沒有因爲聯繫增加了而消失，因此，罪案也是有增無減。在進步的科技之下已可將人體的大部分替換爲生化軀體，且透過埋藏在大腦中的線路，人類意識可以進入數位網路之中。此時出現了許多生化人與網路駭客的新型態犯罪事件，因此成立了直屬於首相的「公安九課」(通稱：攻殼機動隊)，以武裝實力來直接打擊犯罪。本作品對於未來科技的考據、設想，以及精緻細密的描寫，塑造出獨特的世界觀而吸引眾多的科幻愛好者，並對後來的《駭客任務》等許多科幻作品有顯著的影響。

二、從電子政府到電子治理

什麼是「治理」？「治理」一詞非常抽象，主要是指一種政府與被治理者之間的互動模式，涉及公、私部門，以及政策過程中廣大公民社會的組織間合作關係。由於不容易解釋，我們得花一些篇幅，專門解釋這個概念。

[4] 劇情介紹擷取自 http://zh.wikipedia.org/wiki/攻殼機動隊

過去以來，我們比較常聽到「政府」一詞，因爲，政府是我們整個社會中，擁有最多資源、行使公權力的代表，和一般民眾生活息息相關。政府會管制我們的行動、造成我們不便，如不幸遇到警察開罰單、禁止我們未申請的集會遊行、機汽車廢棄超過排放標準的處罰等。同樣地，政府也會提供我們一些特有服務，如消防安檢、治安風水師、免費健檢（預防醫學），以及公園綠帶的闢建等。

「治理」和「政府」有何不同？簡單講，治理概念比較寬廣，治理不僅包含了政府這個角色，還容納了其他角色，包括企業、非營利組織，以及一般公民等。問題是：爲什麼要關注於其他角色呢？如果我們只談論政府，無意中就忘懷了其他角色的功能與價值，這樣一來，我們在關照一些社會問題時，很可能會喪失「想像力」，欠缺問題解決的「撇步」。以老人照護爲例，台灣逐步邁入高齡化社會，老年人口愈來愈多，造就一些社會經濟的問題。過去很長一段時間，這些老人照護的重擔，大多落在地方政府的肩膀上，政府可能要設立安養機構，招募許多考試及格人員，來充任這類服務提供者。老實說，這也沒有什麼不好，政

府是「公家的」，服務會比較有保障。我們不信任政府，還可以信任誰呢？

問題是：我們不也常抱怨政府的不是嗎？在政策上，我們經常覺得政府不能苦民所苦，老是跟人民作對；在服務提供上，我們覺得公務員不是很熱情，不如私人企業（如銀行）般有顧客至上的感受；更糟糕的是，我們有時還會覺得爲什麼非得養這麼龐大的公務人員，不僅效率不高，還有貪腐行爲發生，尤其是報稅時節，這種抱怨聲音更是不絕於耳。

重回老人照護的例子，如果我們從頭到尾只有「政府」這個概念，那麼除了仰賴政府興建更多養老院、雇用更多公務員外，恐怕捉襟見肘、想不出什麼好點子。相對地，如果我們使用的是「治理」這個概念，從政府角色出發，我們可以期待政府充分運用其公權力，設計出一些配套方案，來解決吃重的老人照護問題。這時候，政府可能不需要站在第一線解決問題，而是可以把企業、非營利組織，以及社區組織等，納入問題解決的團隊，彼此集思廣益、責任分擔，來解決高齡化社會普遍面臨的問題。事實上，目前某些基層組織（如里辦公處），這方面就發揮了十足的協調功能。

這類例子太多了，很多與我們日常生活息息相關。回想我們住家附近的鄰里公園，很多是由特定企業負責認養，不是嗎？一些大型硬體建設（如巨蛋、高鐵之類的），也是由民間出資興建，遑論其他軟體建設（如國外監獄、機場營運等），早就不完全由政府來包辦。換言之，當某些本來是

由「政府」直接參與的公共事務，逐漸轉變成只由政府主導，而由民間投入參與者，我們姑且可以把這種現象理解爲「治理」。

爲什麼會出現「電子治理」？和前述比較，其同樣強調政府以外的行動者，共同參與公共事務的處理。不過，比較特別的是，電子治理多了一些「科技因素」帶來的催化效果。譬如說，因爲網路科技的發達，人民可以透過網路完成許多事情。同樣地，在和政府打交道方面，人民可以透過網絡繳交罰單、繳納稅款、申辦服務（如街頭藝人表演證、結婚證書、地籍謄本、租借流動廁所等），以至於寫信給政府抱怨公共服務做得太差等，都含括在內。

簡單來說，從廣義人民的角度（包含企業、非營利組織、社區組織等）出發，所有過去和政府打交道的項目與模式（如選舉投票），皆可能因「資訊與通訊科技」（ICT）的發達與普及，而產生大幅改變的可能。縱使是過去未曾發生、或難以有效發生的交易項目與模式（如市政議題、大型活動舉辦、鄰里建設等），也可能因新科技誕生而有所改觀。就後者而言，當然我們還需要有更多的想像力。

嚴肅地說，政府面對的是廣泛的治理結構轉型，傳統電子化政府的主要任務是透過新的數位平台改善服務遞送效率；如今，因應治理新局的產生，政府與利害關係人關係之重構，遂成爲政府運用資訊通訊科技的首要目標。

三、電子治理的意涵[5]

[5] 此處內容，主要擷取及潤飾自東海大學項靖教授主持之「電子治理關係之調適」委託研究

所謂「電子治理」，可分爲以下層面說明：一如前述，整個社會中，「政府」仍然扮演主要角色，但卻不是唯一角色，因爲舞台上還有許多演員—「多元利害關係人」，他們不再被視爲客體，而是具有能動性，可以主動表達其需求與關切。電子治理最重要是仰賴「資訊與通訊科技」作爲工具，使之融入於治理過程中，包括各種社會關係的經營。電子治理的牽涉層面甚廣，至少包含「公共服務的輸送」、「民眾與政府的溝通」，以及促進整體社會的「公共對話」功能。最後，電子治理造成的影響，有別於傳統比較狹隘的「服務效率」與「政策回應」，而是更加關注於「民主參與」、「透明性」、「課責性」、「公民滿意度」與「信任」等價值。

我們可以這麼比喻：電子治理是運用「資訊與通訊科技」作爲社會變革的工具，致力於改變社會上多元組織與個人之間的交往關係，在這過程中涉入其中的當事者，發覺渠等的影響力迥異於過往，受到對待也大不同於前，因此，逐漸地改變了彼此之間相互依存的關係或認知。

譬如說，你可以想像政府把家戶各類帳單（如水電費、牌照稅、燃料稅，以及手機費等）都統整好，直接掛在網路上供民眾點選，即可完成繳費動作嗎？事實上，中央政府這類服務已經接近成熟。不過，資通科技顯然可以做得更多——試想：倘若鄰里社區的建設，皆能透過地方政府網路平台作爲媒

案期中報告成果。

介，提供民眾表達意見的空間（如停車塔興建、紅黃線劃設、停車格劃設、鄰里公園設施與美化、巷道規劃、路燈式樣、社區治安等），且這樣的意見表示對政府決策（如區公所）構成一定拘束力，您願不願意花點時間關心並表示意見？願不願意投入一些既是個人亦是公共的事務？過去我們缺乏熱忱參與，不乏出於議題無關緊要、表達意見沒有影響力，否則就是不情願撥出時間出席這類討論（如里民大會、公寓大廈管委會等）。但是，現在資通科技發達，社會互動的確可能產生丕變，因爲成本更低廉了。

我們再花一些篇幅闡述「電子治理」的意涵。首先，就多元利害關係人而言，利害關係人是指代表社會中任何的實體（個人、團體、或組織），其可影響或被其他組織執行其目標時所影響。基此，電子化治理的利害關係人，主要包括：公民、公共服務者、企業/社會組織、政府組織、IS/IT的人員、資訊代理人、特殊利益團體。電子治理著重公民主動涉入政治決策過程與運用新科技的參與程度。整體而言，電子治理可被界定爲藉由資訊與通訊科技（ICT）的運用，在國家、企業、公民與非營利組織的不同行動者間，建立水平關係的新治理制度。

其次，就資訊與通訊科技的使用而言，現代資訊與通信科技，尤其是電腦與網路的出現與使用，在人類生活不同面向產生許多改變。資訊與通訊科技（ICT） 改變了人與人之間的互

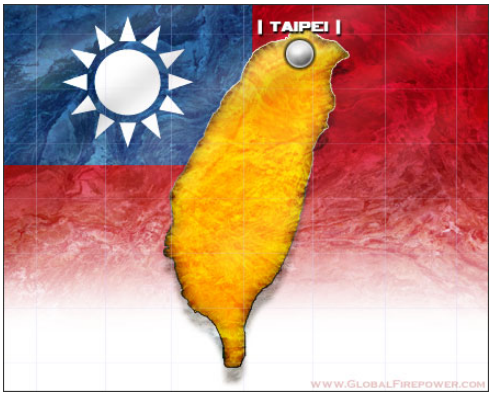
動、以及人與社會整體間的互動方式，新型式的溝通更快速、有效率並有能力接觸社會中的每一個體。新資訊與通信科技的引進，除了帶來電子化政府

的誕生外，更促使現代政府部門出現新的治理型態。電子治理的本質就是利用資訊通訊科技進行治理。政府藉由網際網路的自由便利性，促進訊息流通和電子商務，以增進國家經濟的總體發展以及政府機構相互作用，並且爲公民提供透明參與的系統。

最後，就電子治理的影響層面而言，運用資訊與通訊科技（ICT） 可使政府運作更有效率、減低行政成本、藉此使資訊與政策透明化、並促進公民與政府之間的對話，亦藉此改變公民與政府對於政策制定的產生模式。申言之，電子治理可以視爲一個改變傳統公共服務輸送過程，以及型塑公民與政府之間廣泛互動的一系列科技導向之過程。就改變公共服務輸送過程而言，例如，美、澳洲等國的線上政府（government online）以及單一窗口服務（one-stop shops），其目的在使政府與民眾、企業之間的交易能更容易、便宜、快速、甚至最終可精簡公部門；就型塑公民與政府之間互動而言：係指促進公民參與決策制訂過程，以及提升其直接與政府官員溝通的機會與能力，例如，美國的電子市政廳（electronic town hall）的作法，使公民對話更快速、直接、互動、涵蓋面和參與基礎更廣，可用以教育公民有關的公共事

務和議題，另也包括線上論壇、線上公民投票等；另一方面，藉由電子諮商、電子參與以及政府將公民參與納入考量的意願，並針對特定議題的結果持續提供回饋。

綜合來說，現代資訊與通信科技之發達與應用爲政府治理和公共政策帶來前所未見的影響與契機。資訊與通訊科技（ICT）之應用可視爲一種契機，以促成更廣大的公民參與、公開，且具有課責性的政府、廣泛的意見輸入至政策辯論、以及被充分告知且具有批判能力的公民。總之，在電子治理概念下，效率的促成，需要公民的主動參與才能達成的。因此，電子治理係以政府與公民能夠建立互動、促進服務關係整合、與建立政府與商業公司間更有效率的關係爲目的。



三、台灣電子治理的簡史與案例

（一）台灣電子治理的簡史

早期政府 e 化的努力，最早可追溯自民國 50 年代，斯時部分政府機關即使用資訊技術處理行政業務。官方文件的明確說明，則顯示儘管中央政府各部會推行業務電腦化的時間不一，但普遍在民國 72 年左右設置了各型電腦系統作業。北、高市政府則分別自民國 65 年、68 年，開始逐步推動電腦化作業。至於「全國行政資訊體系」是我國行政資訊建設的基本藍圖，其於民國 72 年完成規劃報告後，即委由相關部會來分頭建置完成。

90 年代初期，爲了因應國家發展，政府推出了國家建設六年計畫，政府部門爲起帶頭作用，因而加速政府業務電腦化工作的推動。行政院資訊發展推動小組的報告書中載明：「爲了配合國家發展，政府業務電腦化將以『提高行政效能，支援國家建設』爲總目標，以提升『服務品質』、『提高行政效率』、『支援政策規劃』及『普及資訊應用』爲政策目標」。

90年代中期以後，相較於先前政府e化速度似乎更爲驚人，每隔幾年方案陸續推陳出新，此一企圖心始自民國86年的「電子化/網路化政府中程（八十七至八十九年度）推動計畫」開始，中經民國90年提出的「電子化政府推動方案（九十至九十三年度）」、「e 化政府計畫（九十二至九十六年度）」，直至去（97）年提出的「優質網路政府計畫（九十七年至一百年度）」，看得出政府在這方面投資是有增無減的。

以最新的優質網路政府計畫爲例，其目標如下：1. 發展主動服務，創造優質生活。2. 普及資訊服務，增進社會關懷。3. 強化網路互動，擴大公民參與打造公民參與資訊平台，提供網路民意互動服務；強化政策資訊公開，方便利害關係人意見陳述，提升決策效能。該階段分別就服務、行政、制度，以及基礎環境等面向進行檢討後，提出如下精進計畫：1. 優質網路政府基礎服務計畫。2. 國家資通安全技術服務與防護管理精進計畫。3. 便捷資訊交換

整合服務計畫。4. 充實基層機關資訊設施及應用計畫。5. 企業e 幫手計畫。6. 民眾e管家計畫。7. 安適e 家園計畫。8. 弱勢e 關懷計畫。9. 政府e 公務計畫。10. 公民e參與計畫。

近十年來，我國電子化政府的推動，已完成政府網路基礎建設與政府網路應用推廣等中程計畫，至今在提升效率及服務品質方面，已具有相當成果。整體而言，我國政府e化的努力方向，明顯從早期「公共事務管理」、「公共服務創新」，逐漸推展至所謂的「公共價值創造」。此三個階段並不能截然二分，而應該視爲一種演進狀態看待。透過政府e化工具及其相關作爲，不僅改變了傳統政府與政府的關係，更重要的是，改變了政府與人民之間的互動關係，以及背後對於民主政治多元價值（如效率、回應、透明等）的體現。

（二）台灣電子治理的案例

1.國家政策網路智庫

國家政策網路智庫就是要達到人民參與、討論的功能。網站規劃時尋遍其他國家的政府經驗，卻沒有一個國家在政策未制定前就提供民眾參與討論的平台。當前，台灣的網路智庫網站可謂是全球首創的民意論壇空間。

圖 3 國家政策網路智庫

資料來源：http://thinktank.nat.gov.tw/mp.asp?mp=1

網路智庫網站最爲特別的是，以往政府的政策在公佈之前沒有一個讓民眾表達意見的平台，日後當主管機關提供研擬中的政策議題時，就會藉由平台意見交流功能，提供相關機關、團體或學者專家研擬建議參考，讓政府機關在政策定案前還有時間修正政策內容，使得制定出來的政策也較趨於完善，透過民意的基礎，也可減輕未來推動的阻力。

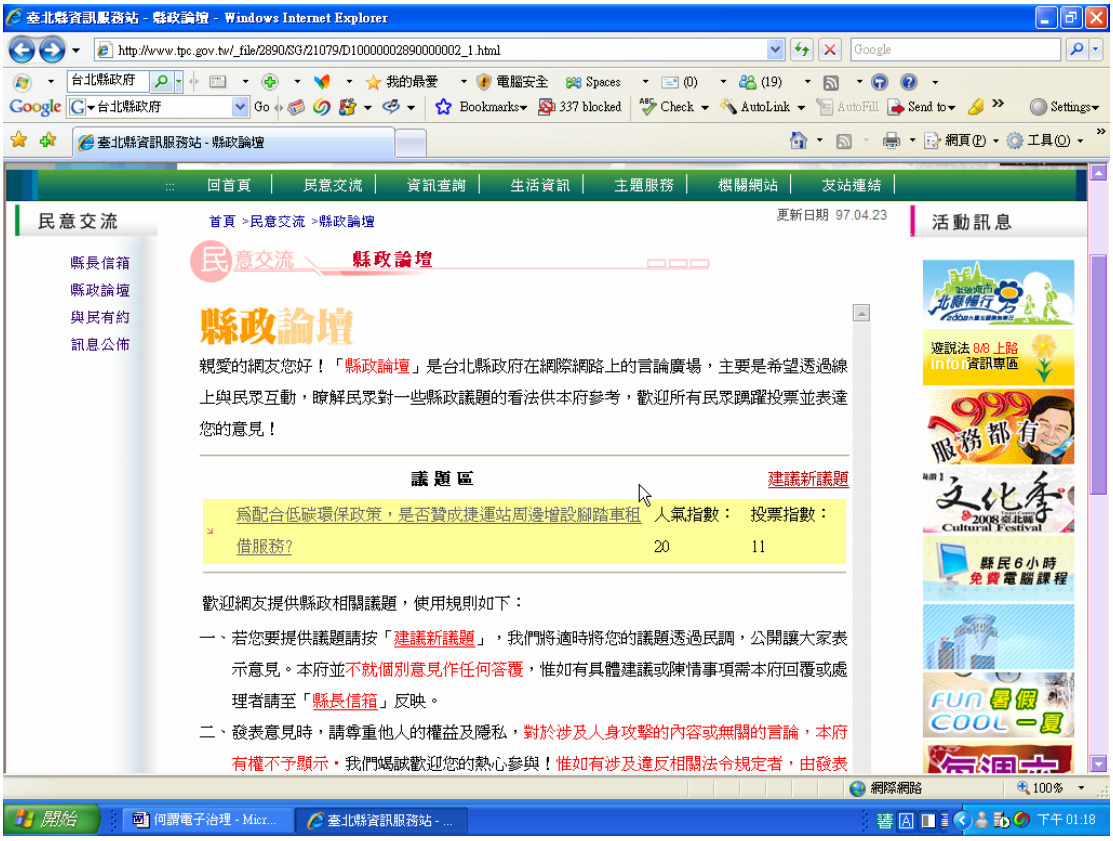
舉例而言，近年來飽受爭議的健保費調漲政策、自動提款機提款金額限

制，以至於油價上漲等政策都引發民眾爭議，常使得民眾認爲政府決策過於草率，且無相關研究以及數據可以支持政策的主張，透過在政策未制定前的討論，將可以讓民眾更了解政府施政過程及背景，幫助政府未來政策施行時更加完善，也達到公民參與的概念。

2.線上論壇

某些地方政府已提供線上論壇服務，讓民眾可以表達施政意見。以台北縣爲例，「縣政論壇」是台北縣政府在網際網路上的言論廣場，主要是希望透過線上與民眾互動，瞭解民眾對一些縣政議題的看法供縣府施政參考。

圖4 線上論壇



資料來源：http://www.tpc.gov.tw/_file/2890/SG/21079/D10000002890000002_1.html

3.行政院公報資訊網

鮮少有人願意投注時間和精力蒐集政府各機關發行的公報，除非與自身權益相關時，才會回過頭尋找主管機關，搜索相關的法規命令，然而訊息繁雜的過程，等到真正用到時，卻不知該從何下手。自從政府電子和紙本公報同步發行後，問題迎刃而解，民眾登錄「行政院公報資訊網」，輸入關鍵字就能找到歷年累積的相關公報資料。從民國91年起，行政院研考會便負起規劃各機關公報整合發行任務，政府資訊透明化時代就此正式展開。

行政院公報資訊網開站以來，每天下午四點即時更新政府法令資訊，因爲資料的即時性和權威性，瀏覽人次有增無減。值得一提的是，爲了主動積極告知最新出刊訊息，行政院公報資訊網還發行中英文電子目次，只要加入會員，每日就能免費收到最新出刊的行政院公報電子目次。

透過行政院公報資訊網，不僅可以即時將政府資訊快速地傳遞到全國，甚至全世界各個角落，而且也提供了民眾和政府間溝通的平台。舉例來說，一般民眾或工商企業可以透過公報資訊網，了解政府最新的法規、命令、政策及各項措施，特別是法規命令、草案預告的刊登，更是與民眾權益息息相關。因此，即時的資訊公布，讓意見回饋和互動機制更加落實，不僅提供政府與民眾直接對話的新管道，也強化施政的程序理性，提升行政效能。

圖5 行政院公報資訊網

資料來源：http://gazette.nat.gov.tw/egFront/index.jsp

4.民眾e管家

工作繁忙、無暇處理生活瑣事是現代人的共同特徵，民眾 e 管家服務打破政府機關被動受理民眾申辦的傳統思維，整合民眾身活切身相關的政府機關與企業服務與資訊，主動即時推播到民眾手中，讓民眾不再遺漏或疏失逾期受罰，是民眾日常生活的好幫手。

爲此，行政院研考會於 96 年度推出「e 管家」各項貼心服務，就是要打造一位 24 小時服務的貼身 e 管家，主動提供水電費、房屋稅、行駕照換照、停車費、汽車定檢、不動產變更等多項通知，還有新生兒預防注射通知等，更創新研發行動 e 管家，讓您隨時隨地打開 PDA 或利用 MSN，就可即時接收各項生活服務訊息。總之，該服務係以「服務到家」主動通知民眾生活訊息，展現政府創新服務方式。

圖 6 民眾 e 管家

資料來源：http://msg.nat.gov.tw/index.aspx

四、國外電子治理的案例[6]

本節將以公共政策的「議程設定」、「規劃」、「執行」與「評估」等重要階段，各介紹一則國外電子治理的案例。

（一）議程設定：非營利組織抗議油價調漲

最近油價上漲，民生物資接連漲價，民眾生活深受其害。我們首先了解一下電子治理可帶給市井小民什麼好處？如何改善市井小民的「發聲」能力？

2000 年秋天英國的鄉下的一個鐵路小站利用網際網路成功抗議英國政府調帳燃料價格。這些抗議者以網際網路集結，採用線上合作與行動通訊方式，成功的以民主的方式表達抗議內容，進而讓立法機關改變政策。

圖 7 非營利團體的政策議程設定網站

[6] 本教材此處內容，主要擷取自江明修、陳敦源、黃東益、莊國容、蕭乃沂等教授主持之「運用資訊與通訊科技實現全民參政理想」之研究成果。

資料來源：http://www.theregister.co.uk/2000/09/13/the_uk_fuel_crisis_all/

該網站以網路註冊方式，網頁的內容呈現出石油議題的相關知識，宣傳石油漲價後的種種影響層面與相關危機，讓關心此議題的網路漫遊者，進一步瞭解議題之後，同聲抗議政府調漲油價。透過網路通訊技術，於短期內迅速而有效率的聚集反對漲價人氣，並隨時透過網際網路溝通與整合網路社群組織，即時傳遞相關的資訊給註冊者，讓小團體累積成巨大的民意力量，影響政府決策而成功的達到抗議目的。

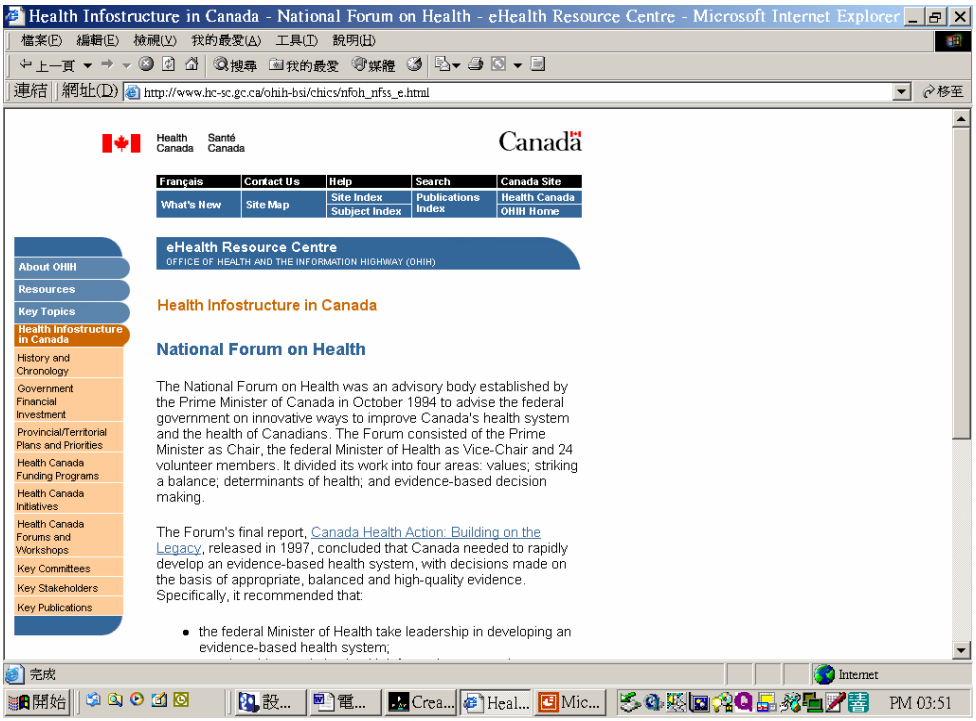
（二）政策規劃：加拿大健保政策的「電子化規劃」（E-planning）

加拿大於 1994 年於內閣總理辦公室之下成立「健保政策國家論壇」（National Forum on Health），並由總理擔任召集人，衛生部長擔任副召集人，負責檢討自從 1950 年代晚期開始實施的全民健康保險（National Health Insurance）政策與整體健康照護政策，並企圖作爲相關措施（如聯邦與各省的健保財務分攤比例、給付範圍調整等）的修正參考，請參考下圖 8。

經過前置規劃之後，健保政策國家論壇決定將整個公民參與過程分爲兩個階段實施。第一階段（約從 1995 年 11 月到 1996 年 4 月）主要在喚起加拿大社會各階層對於健康照護政策的關切，並蒐集各個面向的相關議題。在此階段中，由健保政策國家論壇所委託的民間團體首先負責與各地方相關團體聯繫，並寄出諮商文件作爲召開諮商會議的基礎說明文件。除了實體互動管道之外，健保政策國家論壇也將該諮商文件及已經預定好的會議時程公佈於專屬網站上，以邀請更多的個別民眾與團體參加；對於所有已經召開的諮商會議，也將會議記錄（甚至部份的開會影音實況）公佈於網站上，並提供有興

趣者下載；並且於此專屬網站上開設各相關議題的討論區，使無法參加會議的個別民眾與團體可以發表言論或上傳參考資料；另外工作人員也主動蒐集過程中所有出現於媒體的相關報導，藉以激發更多的線上互動討論。第一階段結束時，全國健康論壇總共召開了 71 場實體的諮商會議，共約 1300 人次參加諮商會議，並累積了可觀的相關言論與參考資料於網站上。在 1996 年 4 月於多倫多舉辦的第一階段綜合研討會中，超過 200 位出席者也依據過程中出現於實體諮商會議與專屬網站的言論（由論壇工作人員整理好於會場上提供出席者），歸納並選擇核心的全民健保與建康照護的待處理議題。

圖 8 加拿大衛生署下的「健保政策國家論壇」

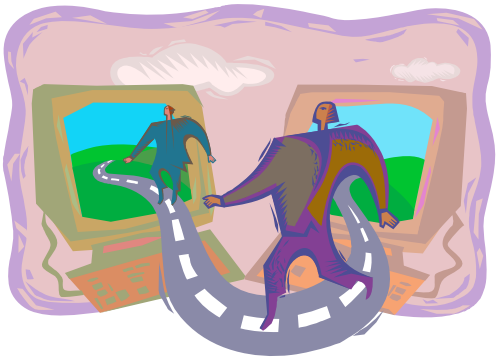


資料來源：http://www.hc-sc.gc.ca/ohih-bsi/chics/nfoh_nfss_e.html

第二階段的目標則是依據前一階段的核心議題，更廣泛地徵詢其解決方案，並作成具體推動措施的優先順序建議。首先，另外兩場於溫哥華及蒙特婁舉行的綜合座談會分別邀集了相關團體的代表、專家學者、與公部門相關部門，針對第一階段的核心議題，羅列代表各方立場的解決方案，並尋求這些解決方案中被綜合研討會的出席者接受的程度。另外，這些解決方案也同時被收納公佈於專屬網站中，並尋求個別民眾透過網路表達其贊同程度（網路投票）或相關評論。於 1996 年秋季，健保政策國家論壇也透過電話民意調查詢問 500 位隨機抽樣的民眾，詢問其對於這些核心議題與對應解決方案的意見，整體而言，這些受訪民眾認爲加拿大的全民健保體制與健康照護措施的確已經有改革的必要，但是對於改革的方案卻無較高的共識。而不論綜合研討會的現場出席者、電話受訪民眾、或是網路參與民眾皆對健保政策國家論壇所設計的公民參與型式感到滿意。

（三）政策執行：美國環境保護署(EPA)電子化管制規則設定(E-rulemaking)

美國聯邦政府自 1980 年代初期開始意識到資訊與通訊科技（ICT）對政府檔案管理以及管制規則設定的工作可能有的影響，經過美國聯邦政府以及國會修法的努力（包括文書減量法以及資訊公開法等），1990 年代開始，美國聯邦政府開始

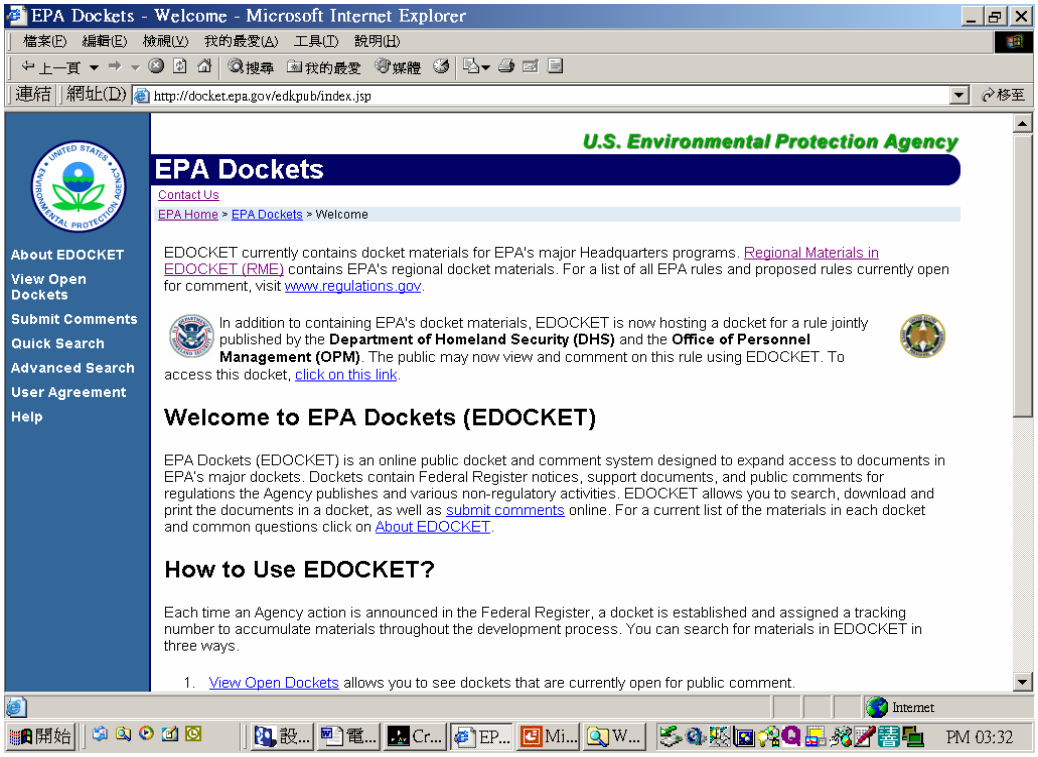


利用網際網路公開政府資訊。1998 年，美國聯邦政府的交通部（the Department of Transportation, DOT）開發了一套線上檔案系統（docket），將部門當中的法令、研究、評論等全數上網，幾年之後，美國環境保護署（the Environmental Protection Agency, EPA）也開發出一套名爲 EDOCKET 的線上檔案系統，這套系統在布希總統的行政管理方案中，成爲推動電子化政府的一個主要項目，其目的是要藉由資訊與通訊科技（ICT）的應用，在資訊公開以及民眾參與的前提之下，提昇政府制定管制規則的品質。之後，美國管理與預算局（Office of the Management and Budget, OMB）指定 EPA 帶領許多聯邦政府的部門開始一項分三階段完成的政府電子化管制規則設定的改善工程，未來美國聯邦政府的任何一條法律命令，都可以在網上輕易取得，民眾也可以對任何一條法律命令，直接在網路上提供意見。

目前 EPA 的 EDOCKET 系統是 2002 年開始上線（如圖 9），它是一個線上公共檔案系統，公民來到這個網址之後，可以藉由搜尋的功能（普通或進階），找到所有與環境保護的法律、命令、管制規則、及其相關政府公文書，舉例而言，筆者於今年六月中進入 EDOCKET 中一則 2004 年 1 月間公佈的「美國國家空氣有毒物質排放標準修正案」，上網最後評論期限是 6 月 29 日，進入該檔案區之後，我們可以看到 3569 個相關檔案（其中大多都有 pdf 供檔下載），檔案性質包括 EPA 的原始提案、其它部會的意見書、研究報告、演講資料、內部備忘錄、其他民眾的意見…，儼然一個該項管制規則改革的臨時圖書館。如果民眾要上傳意見，該系統是以匿名的方式運作，但是系統管

理者仍然希望上傳意見者可以提供聯絡方式，以便於意見傳遞不清時可以聯絡溝通，不然單位無法列入修改提案的考量；另外，系統管理者除了對版權內容、商業機密、以及其他法律禁止的公開文書有權刪除之外，一律來函照登，並列入部門考量；當然，這個公共檔案系統也允許民眾隨時在網上提供與管制政策相關的意見，除了可以履行美國行政程序法中政府管制規則制定，應爲事先告知民眾以及開放評論的要求之外，主要也可達成下列四項目標（Coglianese, 2004: 16）：1.增加民主正當性、2.改進決策品質、3.降低行政成本、4.強化管制的順服等。

圖 9 美國環境保護署線上檔案系統



資料來源：http://docke.epa.gov/edpub/index.jsp

前述的系統仍然在擴充當中，將來發展的方向包括應用資料探勘（data mining）的技術集結更多相關文件以及分析民眾意見、管制規則之間的衝突檢查、對利害關係團體的立即預告系統、管制政策「白話化」（“plain English”）系統、甚至建立「網上公民論壇」（digital juries）以讓民眾對官僚體系關於管制內容的決策有更多的影響力，而「電子化管制規則設定」也漸漸成爲資訊與通訊科技（ICT）在政府政策執行的過程中，最主要的應用場域，不論是學界還是實務界，都有重視發展的聲音出現。

（四）政策評估：法國 D’Europe 計畫-歐洲政策討論版

該計劃與是法國政府與歐盟以五種網站搭配五種論壇的方式建立起來的，該方案提供線上平台討論歐洲共同體的各種政策議題，是一個綜合性、跨越政策領域的政策評估網站，其最重要的目的就是讓一般人民或是利害關係團體，能夠對歐洲共同體所實行的各項政策，提出民眾的看法，彙整之後作爲政策回饋的主要內容，其網站內容主要包括：

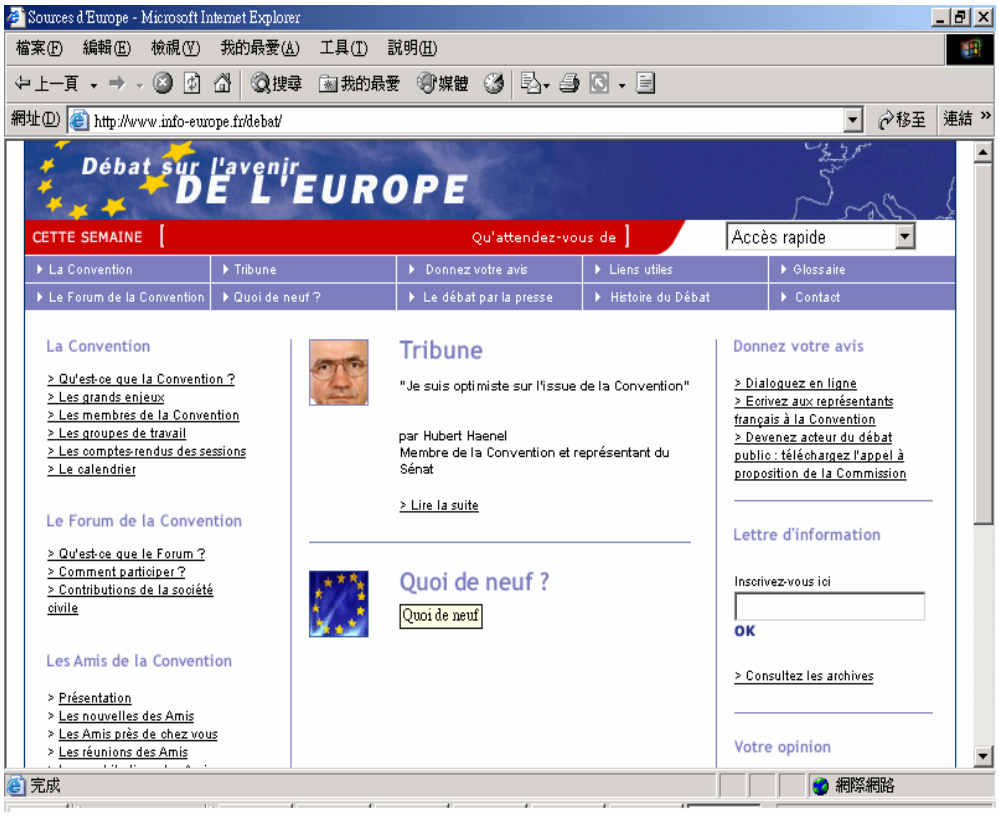
計畫摘要及網站一星期前的所登出的相關討論，主要目的在提供使用者參與討論前便快速的瞭解該議題。

參與五個論壇的民眾之相關知識與意見被視爲有價值的意見並且保證受到該網站主導者的重視，而對於歐盟相關政策具備專業知識的專才，亦會認真看待相關討論並提供建議，因此該網站具備鼓勵資訊交換、教育參與人員的價值，並提供議程設定前的一些小範圍的民意測驗。

根據觀察此網站因爲涵蓋不同的意見與發聲管道，讓參與的人培養包容度。目前此網頁建置的問題：

1. 由於參與網站的人可能是相同的族群而導致重複相同的討論並主導了該項議題。
2. 對於利用此網站表現不滿的民眾意見將不予顯示。
3. 雖然所有的法國境內銷售的名信片均有這五個網站的訊息，但是有論壇主持人抱怨參與的人仍不夠多。

圖 10 法國 D'Europe 計劃的政策討論版面



資料來源：http://www.info-europe.fr/debat/

五、當前資訊科技發展概況

（一）Web 2.0[7]

Web 2.0，是一個新生的術語，它的應用可以讓人了解目前全球資訊網正在進行的一種改變——從一系列網站到一個成熟的爲最終用戶提供網路應用的服務平台。這種概念的支持者期望 Web 2.0 服務將在很多用途上最終取代桌面計算機應用。Web 2.0 並不是一個技術標準，不過它包含了技術架構及應用軟體。它的特點是鼓勵作爲資訊最終利用者透過分享，使到可供分享的資源變得更豐盛；相反的，過去的各種網上分享方式則顯得支離破碎。Web 2.0 是網路運用的新時代，網路成爲了新的平台，內容因爲每位使用者的參與（Participation）而產生，參與所產生的個人化（Personalization）內容，藉由人與人（P2P）的分享（Share），形成了現在 Web 2.0 的世界。

另一方面，其實早在 1999 年，著名的管理學者彼得·杜拉克 (Peter F. Drucker)就曾指出當時的資訊科技發展走錯了方向，因爲真正推動社會進步的，是"Information Technology"裡的"Information"，而不是"Technology"。若然單單著重技術層面而

[7] 內容擷取自維基百科全書，
http://zh.wikipedia.org/w/index.php?title=Web_2.0&variant=zh-tw

忽略了資訊的話，就只是一具空的軀殼， 不能使社會增值。而 Web 2.0 很明顯是透過參與者的互動：不論是提供內容、爲內容索引或評分，都能夠使他們所使用的平台增值。透過參與者的互動，好的產品或資訊本著它的口碑，從一小撮使用者擴展到一大班人，一但超過了臨界質量，就會「像病毒一樣廣泛流傳」(葛拉威爾，2002)。

（二）網誌[8]

網誌（Web log, Blog），又譯爲網路日誌、博客、部落格或部落閣等，是一種通常是由個人管理、定期張貼新的文章、圖像或視頻的網站。

許多網誌對一個特定的課題提供評論或新聞。其他網誌作爲比較個人的日記。一個典型的網誌結合了文字、圖像和通向其他網誌或網站的連接及其它關於主題的媒體。能夠讓讀者在互動的格式下留下意見是許多網址的重要部分。大部分的網誌主要以文字爲主，雖然一些網誌集中在藝術、照片、視頻、音樂、播客，是一個更大的社會媒體網路的部分。網誌有許多種類。種類的區分不只是根據內容，還根據編寫網誌的方法。

[8]內容擷取自維基百科全書，
http://zh.wikipedia.org/w/index.php?title=%E9%83%A8%E8%90%BD%E6%A0%BC&variant=zh-tw

1.個人網誌

個人的持續性的日記或評論，是傳統及最常見的網誌。其作者一般注重網誌的內容，即使他們的網誌從來沒有被除了自己以外的人閱讀過。網誌經常不只是一個溝通的方法，更成爲了一種反映生活的方法或藝術創作。

2.公司網誌

網誌在大部分情況下可以作爲私人用途，但也可以作爲商業用途。用於公司內部以增進聯繫和文化的網誌或對外作爲營銷、品牌的推廣或公共關係目的。

3.依照類型分類

一些網誌集中於某一個特定的課題，如政治網誌、旅遊網誌、居家網誌、時尚網誌、項目網誌和教育網誌。

網誌的出現已經帶來了一連串的法律上的責任和經常無法預見的後果。其中一項備受關注的課題是網誌作者釋放了專有或機密的信息。另一個受到關注的領域是網誌的編寫與誹謗。第三個受到關注的課題是在自己的網誌上寫自己工作的地方或個人生活，因而遭到解僱或其他不利的後果。

（三）輕薄可攜的「電子報」[9]

輕薄可攜帶、有如螢幕、內容不斷更新的電子式報紙閱讀器終於問世。英國「塑膠邏輯」(Plastic Logic)公司八日新推出的「夢幻設備」大小如 A4 影印紙，透過無線連結，可以儲存數百頁報紙、書籍與文件的內容。

國際紙漿、燃油價格飛漲，報紙的生產及運輸成本愈形高昂，而且流通率降低，廣告收入減少，報業老闆莫不叫苦連天。塑膠邏輯公司推出的電子式報紙閱讀器對報界不啻一大福音。塑膠邏輯公司的新設備尚未正式命名，使用的科技與新力公司的「eReader」、亞馬遜網站的「Kindle」相同，都是「電子墨 水」(E Ink)公司研發的顯示器，有黑白兩色、清楚易讀，但塑膠邏輯的電子閱報器卻大上一倍不止；該公司選擇在芝加哥市舉行的新興科技展上公開展出這款閱報器。

[9] 內容擷取自中時電子報，
http://tech.chinatimes.com/2007Cti/2007Cti-News/Inc/2007cti-news-Tech-inc/Tech-Content/0,4703,171705+112008090900302,00.html

塑膠邏輯公司執行長亞裘列塔表示，新推出的設備大小足以刊出報紙版面格式；原本定位爲顯示商業文件之用，但外界最想要的則是電子式閱報器。

塑膠邏輯的電子式閱報器將在二 OO 九年上市銷售。然而，要到 O 九年元月拉斯維加斯「國際消費電子產品展」時，塑膠邏輯才會宣布哪些報社會使用該款閱報器來發布新聞內容。

報界密切觀察電子閱報器科技發展已有很多年。電子墨水公司表示，最理想的型式是像傳統報紙一樣有彈性、可捲曲或折疊的顯示器，這還要過好些年才能研發出來。但該公司副董事長佩魯文巴表示，彩色的超薄顯示器，影像可活動，廣告可點觸互動，再過幾年就能製造出來。

（四）WiMAX[10]

WiMAX （Worldwide Interoperability for Microwave Access，全球互通微波存取），是一項基於標準的技術，主要用在城市型區域網路（MAN）。由 WiMAX 論壇（WiMAX Forum）提出並於 2001 年 6 月成形。它可提供最後一公里無線寬頻接入，作爲電纜和 DSL 之外的選擇。藉由較寬的頻帶以及較遠的傳輸距離，協助電信業者與 ISP 業者建置無線網路的最後一哩，與主要以短距離區域傳輸爲目的之 IEEE 802.11 通訊協定有著相當大的不同。

[10] 內容擷取自維基百科全書，http://zh.wikipedia.org/w/index.php?title=WiMAX&variant=zh-tw

WiMAX 能提供許多種應用服務，包括最後一哩無線寬頻接入、熱點（hotspot）、細胞式回程線路以及企業間的高速連線。通過 WiMAX 一致性測試的產品都能夠對彼此建立無線連接並傳送網際網路封包數據。在概念上類似 WiFi，但 WiMAX 改善了性能，並允許使用更大傳送距離。

WiMAX 達到的頻寬及傳送距離使其具有提供下列服務應用的潛力：

- 作爲 Wi-Fi 熱點間或 Wi-Fi 熱點到達網路其他部分之連接。
- 提供電纜或數位用戶迴路（DSL）以外的無線替代方案。
- 提供高速的行動通訊服務。
- 爲企業營運持續計畫中的網路連線提供多樣化的來源：若企業同時擁有固定及無線網路連接，特別是由不相關的服務供應商提供時，則這些企業將較不易爲特定之服務終止所影響。
- 作爲漫遊連線（Nomadic connectivity）之應用。

（五）3G[11]

第三代行動通訊技術（3rd-generation, 3G），是指以 CDMA2000 爲代表的，支持高速數據傳輸的細胞移動通訊技術。3G 服務能夠同時傳送聲音（通話）及數據信息（電子郵件、即時通訊等）。3G 的代表特徵是提供高速數據業務，速率一般在幾百 kbps 以上。

第一代手機是指類比手機；第二代手機是指數位手機，如我們常見的 GSM 和 cdmarOne（IS-95），提供低速率數據業務；2.5G 是指在第二代手機上提供中等速率的數據服務，傳輸率一般在幾十至一百多 kbps。

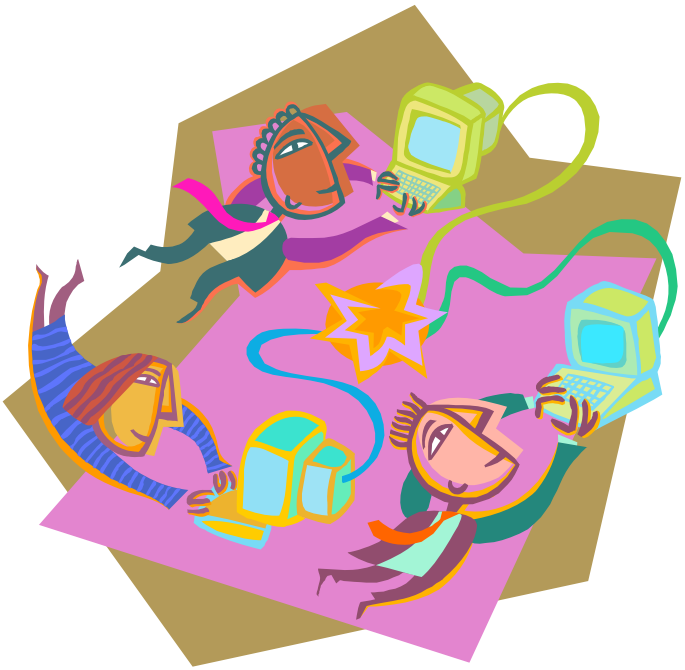
[11] 內容擷取自維基百科全書，http://zh.wikipedia.org/w/index.php?title=3G&variant=zh-tw

3G 能將無線通訊與國際網際網路等多媒體通訊結合的新一代行動通訊系統。能夠處理圖像、音樂、視訊形式，提供網頁瀏覽、電話會議、電子商務信息服務。無線網路必須能夠支持不同的數據傳輸速度，也就是說在室內、室外和行車的環境中能夠分別支持至少 2Mbps、 384kbps 以及 144kbps 的傳輸速度。由於採用了更高的頻帶和更先進的無線（空中介面）接入技術，3G 標準的行動通訊網路通訊質量較 2G, 2.5G 網路有了很大提高，比如軟切換技術使得旅途中高速運動的移動用戶在駛出一個無線小區並進入另一個無線小區時不再出現掉話現象。而更高的頻帶範圍和用戶分級規則使得單位區域內的網路容量大大提高，同時通話允許量大大增加。

肆、劇本介紹

您好，非常歡迎您參與本次「2020 台灣電子治理願景工作坊」，在願景工作坊的進行中，我們將藉由劇本呈現出電子治理在 2020 年所可能出現的各種網路生活景象，下面提供四套劇本，各自代表不同的議題，希望能刺激您對於未來的想像與靈感，進而建構出 2020 年的電子治理願景之面貌。

別忘了「您的想像決定未來網路生活的圖像」，現在就讓我們試著回到未來，去想像各種可能性吧！



一、劇本一

2020 年的台北市是個充滿摩登科技的超現代都市。主角阿福，今年 30 歲，道道地地的台北人，是個年輕有為的勤奮上班族。週末假日的美好時光很快的就過去，又到了星期一的上午，阿福一如往常般要準備出門工作，與平時唯一不同的是今天老婆特別交代要去稅徵處幫忙繳稅，不然就要等著被罰錢了。沒多久準備完畢出門上班去，走在路上，陽光普照，路旁的風景依舊美麗，不禁讓人想起當初求婚的浪漫故事，正當阿福沉醉在美好的回憶時，手機裡卻傳來簡訊的聲音，打開一看，竟然是令人心碎的罰單，原來是星期天出遊時違規停車被發現了，在氣憤之餘，也已經走到公車站牌了，打開手機接收公車和捷運的進站時間，一切都在他的時間掌控之中。沒多久公車果然準時進站，讓他順利搭上捷運避免遲到。

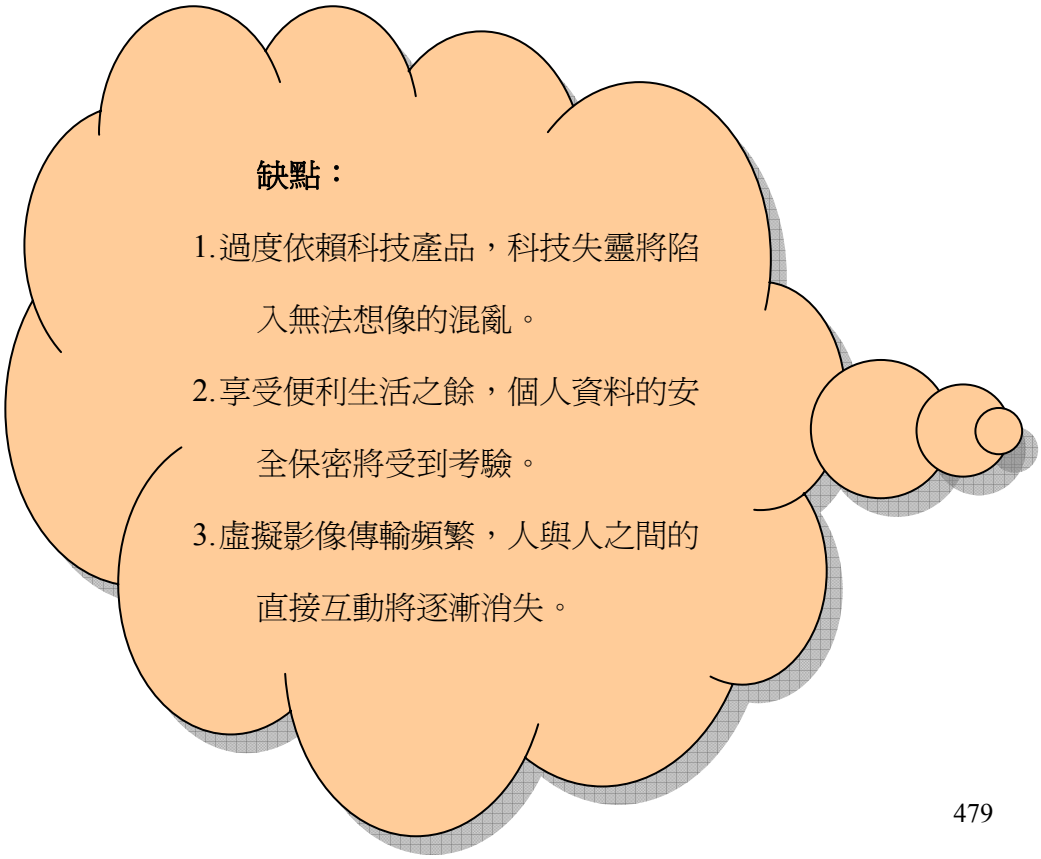
進了公司，大家都忙碌的不得了，老闆還是一樣擺著臭臉在指使大家，阿福在忙碌之餘，也沒有忘記幫家裡買菜；拜科技發達之賜，只要在中午吃飯的休息時間，透過手機就可輕鬆在政府輔導經營農產超市中選取自己想要

的菜色。努力工作了一天，下班時間到了，阿福走出公司突然想起老婆交代要去繳稅的事情，趕緊衝到街角的便利商店繳交稅款，順便偷偷將今早收到的罰單也一併繳了，免得被老婆發現又要被唸一頓！阿福看著便利商店店員親切的服務笑容，心想好在一切政府服務都已電子化，而且各種電子服務都可在各地便利商店即可完成，所以像繳稅這種大事，就算來不及現場繳稅或網路報稅，只要有便利商店就能輕鬆搞定。

繳完了稅和罰單，搭上公車前往和房屋仲介商約好的地點，準備買下人生的第一間房屋，擺脫租屋的日子。到了現場，因爲事先經過看過許多次，這次來是確定要買下這棟別墅。所以很快地就與仲介商談好，便將資料直接傳送到委託的地政士那邊進行處理，過沒多久，阿福就收到由地政士傳來的憑證確認資料，幾乎就在同一時間，手機也收到了由地政事務所和戶政事務所傳來的訊息，通知房屋的過戶已經完成，戶籍的遷移也同時完成了，全部時間竟花不到一小時。阿福看看手錶，也差不多該去接讀國小的小孩了，在安親班的門口看到小孩天真可愛的笑容，一整天的疲勞完全一掃而空。

坐上公車在回家的路途中，小兒子從書包前袋中拿出電子連絡簿，阿福打開看到老師的

留言影像通知星期六要開家長會和說明小孩今天在學校的狀況，而寶貝兒子也很乖地在一旁使用上個月媽媽買給他的超薄電子紙，複習著今天的作業；在回覆完老師的訊息後，沒一會兒也到站了。牽著小兒子的手踏上回家的路程，一路上回想著今天的行程之所以能如此順利，科技占了關鍵的地位，因爲科技的發達讓政府許多事務能更輕鬆快速的完成，使得我們的個人生活也變得更加便利了。一轉眼已經到了家門口，一開門映入眼廉的是外婆從屏東用電子郵務系統宅配寄來的萬巒豬腳，上面還有著外婆個人的電子影音郵票。經過一番休憩，在餐桌上啃著豬腳的阿福，此時心中充滿了家庭的幸福與外婆親切的笑容，讓他一邊享用美食，一邊和家人分享著科技發展造就便利生活的種種好處….



優點：

1.民眾不用排隊等待或使用繁雜的網路進行報稅或繳費。

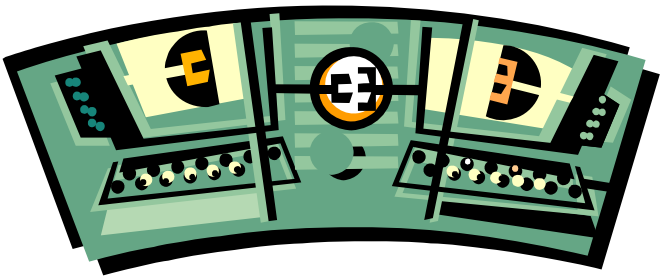
2.即時的政府資訊傳遞，民眾得以隨時掌握所需的生活資訊。

3.快速資料往返，個人生活不再因政府上班時間的固定所苦。

4.即時影音傳送，虛擬影像帶來無限感動，溝通更快速、便利。

二、劇本二

2020 年的科技發展超乎想像，DNA 之謎已經慢慢解開，而每位國民也可在個人同意之後免費建置專屬的 DNA 資料庫，並納入「電子病歷法」的規範，政府以及任何人均不得非法取得他人的 DNA 資料，最近則有一份頗具爭議的英國研究指出，具有「Z 基因」的人工作效率較一般人來得差，引起各企業的熱切關注…

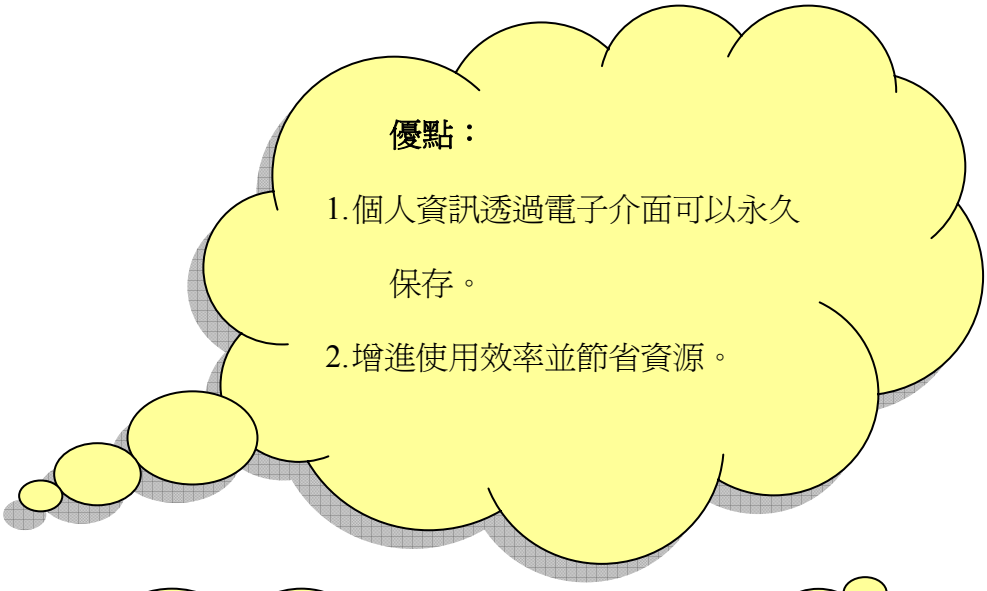


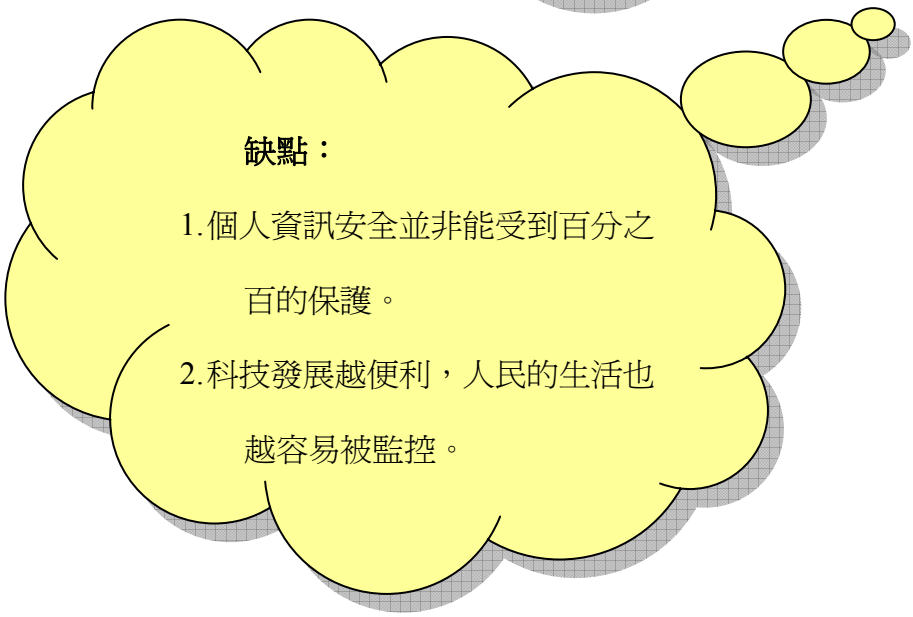
「小美～快點起床囉！今天是工作面試的日子，可別遲到了唷！」小美的媽媽七早八早就在客廳大喊著。

小美在媽媽的吶喊中驚醒，趕緊起身梳妝打理後，便用了指紋辨識器打開電腦確認自己今天的面試行程，心想今天面試一定要加油找個好工作。22 歲的小美，今年剛大學畢業，是位準備踏入職場的社會新鮮人，雖然在校成績優異，每次投履歷都有面試機會，但是自從畢業之後找工作卻一直碰壁，她自認面試表現不差，卻一直不被錄用讓她想不透究竟問題出在哪裡。

今天預定要去三家公司面試，來到了第一家公司之後，小美也很熟悉地在公司人事部將自然人憑證 IC 卡放在感應區前，讓對方確認自己的身分。原來 2020 年每位國民都配有一張高科技的感應式自然人憑證 IC 卡，這張卡片整合了身分證以及健保卡只要把它放在電腦前的感應區，輸入個人密碼即可確認個人身分，省去影印的麻煩以及紙資源的浪費。就這樣今天結束了三家

公司的面試之旅，晚上回到家準備開信箱查看有沒有錄取通知，這時候晚間新聞播放今日頭條，標題寫著「檢方破獲史上最大宗醫療弊案，個人病歷全都露」，讓始終無法被錄取的小美不禁擔心起來...。





三、劇本三

西元 2020 年，國人 GDP 已達 3 萬美元，新興資訊與通訊科技（ICT）技術更快速的發展，人人享受全面數位化的家庭生活，使用智慧型車輛代步、家事則由簡易型機器人代勞，藉由跨領域技術間的融合，IT 與 BT 結合研發出了 DNA 生物晶片（BIO-CHIP），除了安全防禦外也應用於醫療診檢，政府更以免費植入晶片作爲銀髮族照護政策，而衛生署與資策會合併，致力於疾病與環境健康的防治。政府成立「台灣無疆界部」負責政府部門與第三部門間的工作整合，民眾有疑難雜症都可以逕在「無疆界部」網站留言陳述，隨即「無疆界部」即會派相關的機關單位人員連絡並處理。

大雄爲剛退休的中學教師，剛剛才在「無疆界部」網站留下對台中大肚溪老家溪畔設置的垃圾掩埋場，有任意燃燒惡臭廢棄物的質疑訊息，隨即家用電視上傳來了「無疆界部」要求即時影音通訊 5 分鐘的字幕，在電視共用螢幕上，有「無疆界部」的陳姓受理人員、河川署台中烏日段的負責人，

以及彰化縣環保局稽查人員透過影音直接聽著大雄抱怨，並且各自記下職責所屬事項，並向大雄約定好由「無疆界部」回覆最後結果，然而就在大雄要向承辦人員道謝時，發生了規模 7.8 的大地震！在一陣天搖地動後，大雄家竟然全倒！這時「無疆界部」隨即按下橙色災變按鈕，其所屬的 NPO 小組自動與各地慈濟功德會、法鼓山與基督教分會等連線，發起救災準備，而同一時間，住在大雄隔壁的里長，拿出每一里都有配置的晶片掃瞄器，透過定位後，終於順利救出了瓦礫堆下慶幸自己撿回一命的大雄…。

優點：

1.沒有組織界線作梗，民眾可以更有效率的滿足多元需求。

2.合作平台增加，社會資本增多。

缺點：

1.部門間的本位主義衝突。

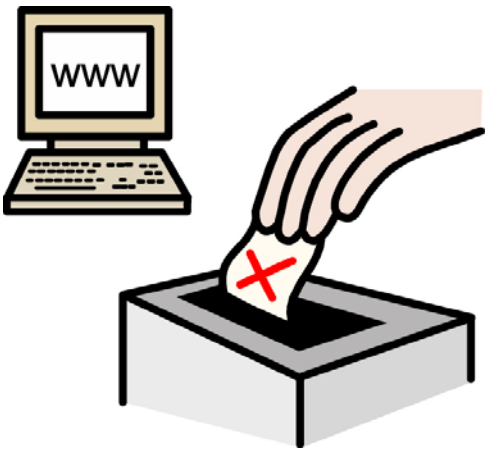
2.組織界線的模糊，責任難以歸屬。

3.參加者眾多，增加協商成本。

四、劇本四

「全民政府」在過去是大家而熟能詳的政治口號，然而到了 2020 年政府已經透過先進的網路資訊科技建立出新一代的全民政府，透過網路坐在家裡，人人都是國策顧問和諮詢委員，甚至，投票只要在家連線動動手指就可以完成，專家學者們都說這是二十年前「優化民主」（ubiquitous democracy）的理想實踐，但是…

2020 年的某一天，剛滿二十歲的大學生小明上完課準備回家，在便利商店中的 LED 資訊布告欄，看見由近來最紅的新世紀樂團代言的廣告，以該團成名曲「We Need You」，提醒民眾把握「台灣高速鐵路網是否應該延伸到澎湖」公投的最後兩天，記得上網投票，小明這才想起自己剛滿二十歲，應該可以行使投票權了，小明立刻拿起手中的手機，打開高速行動通訊上網，找尋與公共事務相關的訊息，在MSN-2 中剛巧也收到一封來自政府的通知訊息，提醒他爲期一週的網路公投尚未投票，並且告知若是第一次參與網路公投，下個月高速網路費用可享有八折優待的好康，訊息的最下方附有公投議題的說明與投票連結，並附有小明專屬的投票通關密碼。小明看了一下公投的內容，雖對這次公投議題不感興趣，但是想到下月網路費用可享有八折優待，投個公投倒也不無小補，



正打算從政府的訊息留言中連結到投票網頁的時候，MSN-2 卻傳來一則不尋常的廣告訊息...「別傻了，網路八折？你的一票可以更值錢！」小明不禁被這樣聳動的標題吸引住目光，點進去一看原來是某不知名集團打算以一萬元的代價收購自己的自然人憑證密碼跟此次公投的通關密碼…。

優點：

1. 降低公民參與的成本
2. 擴大並提昇公民的實質參與

缺點：

1. 等同對資訊能力不足或是缺乏設備的民眾形成不平等。
2. 投票者身分曝光以及賄選買票的問題。

附錄十九 2020 台灣電子治理願景工作坊專題演講簡報資料