NIST Cyber Security: Legislative Update

Ed Roback
Chief, Computer Security Division
edward.roback@nist.gov

National Institute of Standards and Technology NIST

Agenda

1. **Homeland Security Department**
2. **Cyber Security Research and Development Act**
3. **Federal Information Security Management Act**

Homeland Security Act

11/25/2002 Became Public Law No: 107-296.

DIRECTORATE FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

UNDER SECRETARY OF HOMELAND SECURITY FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

ASSISTANT SECRETARY FOR INFORMATION ANALYSIS;

ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION

Functions Transferred:

(1) The National Infrastructure Protection Center of the Federal Bureau of Investigation

(2) The National Communications System of the Department of Defense

(3) The Critical Infrastructure Assurance Office of the Department of Commerce,

(4) The National Infrastructure Simulation and Analysis Center of the Department of Energy and the energy security and assurance program and activities of the Department

(5) The Federal Computer Incident Response Center of the General Services Administration

Cyber Security Research and Development Act

Signed into Law by President Bush on 11-27-2002

Cyber Security Research and Development Act

- National Science Foundation
  - grants for basic research
  - support for higher education (many variants)
- NIST
  - research grants
  - cyber security checklists
  - in-house research:
    - Composability; SCADA; long-term/high-risk
  - Advisory Board and NRC study

Research Support

- to institutions of higher education that enter into partnerships with for-profit entities to support research to improve the security of computer systems
- Grants or Cooperative Agreements

Fellowships

- Post-Doctoral Research
  - engaged in research activities related to the security of computer systems
- Senior Research
  - individuals seeking research positions at institutions, including NIST
  - for established researchers at institutions of higher education who seek to change research fields and pursue studies related to the security of computer systems

Intramural Research

- emerging technologies associated with assembling a networked computer system from components while ensuring it maintains desired security properties;
- improving the security of real-time computing and communications systems for use in process control; and
- multidisciplinary, long-term, high-risk research on ways to improve the security of computer systems.

Expanded Role of Board

- to identify research topics for the NIST grants to higher institutions (in accordance with the Act, Section 8a), including research needs related to computer security, privacy, and cryptography
- provide for the Board, as appropriate, to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.

NRC Study

- Section 12 of Act
- NIST arrange with the National Research Council
- study of the vulnerabilities of the Nation's network infrastructure
- make recommendations for appropriate improvements.

Cyber Security Checklists

- Definition –

  a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal government.
- NIST would set priorities for development

Agency Use of Checklists (1)

- The Act does **NOT:**
  - require agencies to select the specific settings or options recommended by the checklist for the system;
  - establish conditions or prerequisites for Federal agency procurement or deployment of any such system;
  - represent an endorsement of any such system by NIST ; nor
  - preclude agencies from procuring or deploying other computer hardware or software systems for which no such checklist has been developed.

Agency Use of Checklists (2)

- If an agency uses a system for which a checklist is issued, the agency:
  - shall include in their program plan an explanation of how the agency has considered such checklist in deploying that system; (except for national security systems) and
  - may treat the explanation as if it were a portion of the agency's annual performance plan properly classified under criteria established by an Executive Order (within the meaning of section 1115(d) of title 31, United States Code).

Funding *Authorizations*

- Research Assistance and Fellowships
  - FY-03 $25,000,000
  - FY-04 $40,000,000
  - FY-05 $55,000,000
  - FY-061 $70,000,000
  - FY-07 $85,000,000
- Checklists
- Intramural Research
  - FY-03 $6,000,000
  - FY-04 $6,200,000
  - FY-05 $6,400,000
  - FY-061 $6,600,000
  - FY-07 $6,800,000
- Board
  - FY-03 $1,060,000
  - FY-04 $1,090,000
- NRC Study - $700,000

Federal Information Security Management Act (HR 2458)

Title III of E-Government bill

(Status: passed House and Senate 11-15)

Purpose

- Provide Leadership in Promoting Electronic Government
- Promote Interagency Collaboration
- Utilize Best Practices and Technologies from Public and Private Sector Organizations
- Promote Enhanced Access to Government Information Consistent with Required Protections
- Provide Greater Agency Assistance

NIST Role

Establishes an Information Technology Framework Based on NIST Standards

Continuing Key Areas:

Developing security standards, guidelines, and associated methods and techniques for information services

Conduct security research – understand vulnerabilities and develop new security techniques

New Key Areas:

1 Developing information categorization based on levels of sensitivity

"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"

12 month time-line

Status: See 800-37 draft.

Comments:

New Key Areas:

2 Developing guidelines for information classification for each category

"guidelines recommending the types of information and information systems to be included in each such category"

18 month time-line

Status:

Comments: Agency workshop(s) a necessity.

New Key Areas:

3 Developing minimum security requirements by category

"minimum information security requirements for information and information systems in each such category"

36 month time-line

Status: Draft 800-53A now in development (Spring 2003)

Comments: Validation procedures follow-on activity; voluntary organizational conformance program – an open question

New Key Areas:

4 Incident detection and handling guidelines

"a definition of and guidelines concerning detection and handling of information security incidents"

Status: Goal of –04/Q1 draft.

Comments: Will need close coordination with DHS-FedCIRC

New Key Areas:

5 Assistance – Agencies and Private Sector

- Provide technical assistance to agencies, upon request, regarding:

– compliance with the standards and guidelines

– detecting and handling information security incidents

- Provide assistance to the private sector, upon request, in using and applying the results of activities …

Status:

Comments: NIST conducts substantial reimbursable and non-reimbursable assistance support

New Key Areas:

6 Developing performance indicators/ metrics

"develop and periodically revise performance indicators and measures for agency information security policies and practices"

Status: See draft 800-55; **Security Metrics Guide for Information Technology Systems**

Comments:

New Key Areas:

7 Evaluating security policy and technologies for federal use – private sector and national security systems

Evaluate private sector information security policies and practices, security policies and practices developed for national security systems, and commercially available information technologies to assess potential application by agencies to strengthen information security

Status: technology evaluation operational– NIAP & CMVP

Comments: Policy/practices – new

New Key Areas:

8 Identification of national security systems guidelines

"guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system"

Status:

Comments:

Other Requirements

- consult with other agencies to (1) avoid duplication, et al; and (2) complementary with national security systems
- provide the public with an opportunity to comment on proposed standards and guidelines
- avoid use or procurement of specific products
- allow for flexibility for alternate solutions
- use performance-based standards
- submit such standards to the Secretary with recommendations as to extend of "mandatory applicability"
- Annual NIST reporting requirement
- solicit recommendations of the Board on draft standards and guidelines

Advisory Board

- re-named "Information Security and Privacy Advisory Board"

- Augments Mission:

  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

- Annual Board reporting requirement

Funding *Authorizations*

NIST FISMA Activities

FY-03	$20,000,000
FY-04	$20,000,000
FY-05	$20,000,000
FY-6	$20,000,000
FY-07	$20,000,000

Board

General provision – such sums as may be necessary