

2018 Current Fiscal Year Report: Information Security and Privacy

Advisory Board

Report Run Date: 06/19/2019 02:44:01 PM

1. Department or Agency

Department of Commerce

2. Fiscal Year

2018

3. Committee or Subcommittee

Information Security and Privacy Advisory Board

3b. GSA Committee No.

324

4. Is this New During Fiscal Year?

No

5. Current Charter

03/02/2018

6. Expected Renewal Date

03/02/2020

7. Expected Term Date

8a. Was Terminated During Fiscal Year?

No

8b. Specific Termination Authority

8c. Actual Term Date

9. Agency Recommendation for Next Fiscal Year

Continue

10a. Legislation Req to Terminate?

No

10b. Legislation Pending?

Not Applicable

11. Establishment Authority

Statutory (Congress Created)

12. Specific Establishment Authority

15 U.S.C. 278g-4

13. Effective Date

01/08/1988

14. Committee Type

Continuing

14c. Presidential?

No

15. Description of Committee

Scientific Technical Program Advisory Board

16a. Total Number of Reports

No Reports for this Fiscal Year

17a. Open Meetings 3 17b. Closed Meetings 0 17c. Partially Closed Meetings 0 17d. Total Meetings 3

Meetings and Dates

Purpose	Start	End
Advise the Secretary of Commerce, the Director of the National Institute of Standards and Technology (NIST), and the Director of the Office of Management and Budget (OMB) on information security and privacy related issues. The Board' agendas of these meetings are established based on the Board's work list of emerging issues that has been developed and is reviewed and updated at every meeting. The meeting agenda topics also include non-work list items that are considered by the board of immediate security and privacy concerns to the federal government information systems. The invited presenters at every Board meeting were leaders and experts from private industries, academia, federal agency CIOs, IGs and CISOs.	10/25/2017	10/27/2017
Advise the Secretary of Commerce, the Director of the National Institute of Standards and Technology (NIST), and the Director of the Office of Management and Budget (OMB) on information security and privacy related issues. The Board' agendas of these meetings are established based on the Board's work list of emerging issues that has been developed and is reviewed and updated at every meeting. The meeting agenda topics also include non-work list items that are considered by the board of immediate security and privacy concerns to the federal government information systems. The invited presenters at every Board meeting were leaders and experts from private industries, academia, federal agency CIOs, IGs and CISOs.	03/15/2018	03/16/2018

Advise the Secretary of Commerce, the Director of the National Institute of Standards and Technology (NIST), and the Director of the Office of Management and Budget (OMB) on information security and privacy related issues. The Board' agendas of these meetings are established based on the Board's work list of emerging issues that has been developed and is reviewed and updated at every meeting. The meeting agenda topics also include non-work list items that are considered by the board of immediate security and privacy concerns to the federal government information systems. The invited presenters at every Board meeting were leaders and experts from private industries, academia, federal agency CIOs, IGs and CISOs.

06/21/2018 - 06/22/2018

Number of Committee Meetings Listed: 3

	Current FY	Next FY
18a(1). Personnel Pmts to Non-Federal Members	\$0.00	\$0.00
18a(2). Personnel Pmts to Federal Members	\$0.00	\$0.00
18a(3). Personnel Pmts to Federal Staff	\$26,074.00	\$48,000.00
18a(4). Personnel Pmts to Non-Member Consultants	\$0.00	\$0.00
18b(1). Travel and Per Diem to Non-Federal Members	\$7,366.00	\$10,000.00
18b(2). Travel and Per Diem to Federal Members	\$0.00	\$0.00
18b(3). Travel and Per Diem to Federal Staff	\$364.00	\$1,000.00
18b(4). Travel and Per Diem to Non-member Consultants	\$0.00	\$0.00
18c. Other(rents,user charges, graphics, printing, mail, etc.)	\$48,245.00	\$50,000.00
18d. Total	\$82,049.00	\$109,000.00
19. Federal Staff Support Years (FTE)	0.50	0.50

20a. How does the Committee accomplish its purpose?

The Information Security and Privacy Advisory Board's statutory purpose is to advise the Secretary of Commerce, the Director of the National Institute of Standards and Technology (NIST), and the Director of the Office of Management and Budget (OMB) on information security and privacy related issues. The Board meets 3-4 times a year, and the agendas of these meetings are established based on the Board's work list of emerging issues that has been developed and is reviewed and updated at every meeting. The meeting agenda topics also include non-work list items that are considered by the board of immediate security and privacy concerns to the federal government information systems. The invited presenters at every Board meeting were leaders and experts from private industries, academia, federal agency CIOs, IGs and CISOs. An annual report is submitted and included in NIST Special Publication 800-176 Computer Security Division Annual Report

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-176.pdf>. During this fiscal year, the board submitted three recommendation letters to OMB and NIST relating Mobile Device and Derived Credentials, Department of Commerce Review Risk Management Process, and Realignment within NIST's Information Technology Laboratory (ITL) - adding another division devoted to cybersecurity.

20b. How does the Committee balance its membership?

The Board is comprised of members from a broad range of interested parties. There are three main categories and each category has four members. Category 1 includes members from outside the Federal government eminent in the information technology industry, at least one of whom is representative of small or medium-sized companies in such industries. Category 2 also includes members from outside the Federal government and not employed by or representative of a producer of information but are eminent in the field of information technology, or related disciplines. Category 3 includes members from the Federal government who have information system management experience, including experience in information security and privacy, at least one of whom should be from the National Security Agency. Federal members bring a detailed understanding of the Federal processing environment; industry brings concerns and experiences regarding product development and market formation, while private computer security experts are able to bring their experiences of commercial cost-effective security measures into Board discussion. Presently, the membership of the Board consists of eleven members including Chairperson. Late September, the Board lost one member (Federal) due to job changed, but added a new member in Category 2.

20c. How frequent and relevant are the Committee Meetings?

The Board holds open, public meetings 3-4 times a year. At the first meeting of every fiscal year i.e. October 2017, the Board reviewed and updated its work plan items for FY2018. The list includes: NIST Cryptography process, measuring outcomes from information sharing and gaps, design plan to raise NIST profiles and trust, issues relating to quantum, identity management and derived credential, privacy and ways for implementors and testing, medical devices safety and privacy, continuous diagnostic monitoring and cybersecurity Framework.

20d. Why can't the advice or information this committee provides be obtained elsewhere?

In drafting the Computer Security Act of 1987, which created this Advisory Board, we understand that Congress saw a need for an independent, non-federally dominated group of computer security experts to offer its advice to senior government officials on emerging computer security areas. The Board members, with their individual and collective skills, responsibilities and experiences fulfill this requirement. No other similar group of experts meet regularly to review information security issues involved in unclassified Federal Government computer systems and networks. In today emerging technology, privacy is ever moving into prominent importance not just for security but in bring about confidence from industry and consumers. Also, Title III of the E-Government Act of 2002 reaffirmed the need for this Board by giving it additional responsibilities.

20e. Why is it necessary to close and/or partially closed committee meetings?

N/A

21. Remarks

Cost is significantly lower due to the cost-drop in facility/meeting location cost as well as not having a federal employee assigned to this committee for most of the fiscal year. No annual report has been provided by the Board as there has been no changes from the previous year's report. Jacob Daniel Toler resigned from ISPAB at the end of FY16. Laura Delaney replaced Mr. Toler in June 27, 2017.

Designated Federal Officer

Jeffrey Brewer DFO

Committee Members	Start	End	Occupation	Member Designation
Anton, Ana	11/04/2015	11/03/2019	Professor	Special Government Employee (SGE) Member
Baker, Brett	03/15/2018	03/14/2022	Assistant Inspector General for Audit, Nuclear Regulatory Commission	Regular Government Employee (RGE) Member
Boyer, Christopher	06/11/2012	06/10/2020	Assistant Vice President, Public Policy, AT&T Services Inc.	Special Government Employee (SGE) Member
Centafont, John	11/26/2013	02/27/2019	National Security Agency	Regular Government Employee (RGE) Member
Delaney, Laura	06/27/2017	05/15/2019	Deputy Director DHS	Regular Government Employee (RGE) Member
Garcia, Gregory	11/03/2011	11/02/2019	Principal, Garcia Cyber Partners	Special Government Employee (SGE) Member
Greene, Jeffrey	10/27/2015	10/26/2019	Director, Government Affairs N.America & Senior Policy Counsel	Special Government Employee (SGE) Member
Groman, Marc	09/12/2017	09/11/2021	Senior Advisor for Privacy, The White House	Regular Government Employee (RGE) Member
Hatter, Patricia	09/14/2016	09/13/2018	Intel Corporation	Special Government Employee (SGE) Member
Lipner, Steven	05/31/2018	05/30/2022	Executive Director, Safecode	Special Government Employee (SGE) Member
Roback, Edward	03/28/2011	03/27/2019	Associate CIO for Cybersecurity and CISO, US Department of Treasury	Regular Government Employee (RGE) Member

Number of Committee Members Listed: 11

Narrative Description

The Board advised NIST, the Secretary of Commerce and the Director of OMB on information security and privacy issues pertaining to Federal government unclassified information systems. This includes thorough review of proposed standards and guidelines developed under Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) as amended by Title III of the E-Government Act of 2002.

What are the most significant program outcomes associated with this committee?

Checked if Applies

- Improvements to health or safety
- Trust in government
- Major policy changes
- Advance in scientific research
- Effective grant making
- Improved service delivery
- Increased customer satisfaction
- Implementation of laws or regulatory requirements
- Other

Outcome Comments

NA

What are the cost savings associated with this committee?

Checked if Applies

- None
- Unable to Determine
- Under \$100,000
- \$100,000 - \$500,000
- \$500,001 - \$1,000,000
- \$1,000,001 - \$5,000,000
- \$5,000,001 - \$10,000,000
- Over \$10,000,000
- Cost Savings Other

Cost Savings Comments

Many of the recommendations address information security and privacy policy government-wide. Cost savings would vary based on agency-specific implementation.

What is the approximate Number of recommendations produced by this committee for the life of the committee?

38

Number of Recommendations Comments

Since the first year through this fiscal year, the Board submitted a total of 36 recommendations. During FY 2014, the Board submitted three recommendation letters <http://csrc.nist.gov/groups/SMA/ispab/documentation.html> to OMB and worked closely with NIST on Executive Order for Cybersecurity Framework and on reviewing NIST

Cryptography process. In 2014/5, the Board submitted three letters of recommendation to OMB, the Secretary of Department of Commerce, and NIST Director: 1) Mobile Device and Derived Credentials, 2) Department of Commerce Review Risk Management Process, and 3) Realignment within NIST's ITL - adding another division devoted to cybersecurity.

What is the approximate Percentage of these recommendations that have been or will be Fully implemented by the agency?

29%

% of Recommendations Fully Implemented Comments

All recommendations do not address the agency. They may be directed to OMB for government-wide impact, which is difficult to report or monitor percentage of implementation. Those time lines are driven by the OMB directives. Board recommendations specific to NIST have been or will be addressed and implemented.

What is the approximate Percentage of these recommendations that have been or will be Partially implemented by the agency?

0%

% of Recommendations Partially Implemented Comments

NA

Does the agency provide the committee with feedback regarding actions taken to implement recommendations or advice offered?

Yes No Not Applicable

Agency Feedback Comments

Feedback to the Advisory Board are filtered in several ways: oral communications with the membership, status presentations to the Board, email communications, formal reply to recommendations and the use of a dedicated web-site.

What other actions has the agency taken as a result of the committee's advice or recommendation?

Checked if Applies

- Reorganized Priorities
- Reallocated resources
- Issued new regulation
- Proposed legislation

Approved grants or other payments

Other

Action Comments

NIST has refined their strategy based on objective feedback related to presentations and submissions of the Board.

Is the Committee engaged in the review of applications for grants?

No

Grant Review Comments

NA

How is access provided to the information for the Committee's documentation?

Checked if Applies

Contact DFO

Online Agency Web Site

Online Committee Web Site

Online GSA FACA Web Site

Publications

Other

Access Comments

Information is published in the FEDERAL REGISTER announcing the meetings and agendas and announcing an annual request for nomination consideration to the membership of the Board.