

## 2024 Current Fiscal Year Report: Information Security and Privacy Advisory Board

Report Run Date: 04/19/2024 08:15:38 PM

### 1. Department or Agency

Department of Commerce

### 2. Fiscal Year

2024

### 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

02/23/2024

### 6. Expected Renewal Date

02/23/2026

### 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?

Not Applicable

### 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

2

17b. Closed

0

17c. Partially Closed

0

Other Activities

0

17d. Total

2

### Meetings and Dates

Purpose

Start

End

The Information Security and Privacy Advisory Board (ISPAB) is authorized by 15 U.S.C. 278g-4, as amended, and advises the National Institute of Standards and Technology (NIST), the Secretary of Homeland Security (DHS), and the Director of the Office of Management and Budget (OMB) on information security and privacy issues pertaining to Federal government information systems, including through review of proposed standards and guidelines developed by NIST.

10/25/2023 - 10/26/2023

The Information Security and Privacy Advisory Board (ISPAB) is authorized by 15 U.S.C. 278g-4, as amended, and advises the National Institute of Standards and Technology (NIST), the Secretary of Homeland Security (DHS), and the Director of the Office of Management and Budget (OMB) on information security and privacy issues pertaining to Federal government information systems, including through review of proposed standards and guidelines developed by NIST.

03/20/2024 - 03/21/2024

#### Number of Committee Meetings Listed: 2

|   | Current<br>FY | Next<br>FY |
|---|---------------|------------|
| <b>18a(1). Personnel Pmts to Non-Federal Members</b>                  | \$0.00        | \$0.00     |
| <b>18a(2). Personnel Pmts to Federal Members</b>                      | \$0.00        | \$0.00     |
| <b>18a(3). Personnel Pmts to Federal Staff</b>                        | \$0.00        | \$0.00     |
| <b>18a(4). Personnel Pmts to Non-Member Consultants</b>               | \$0.00        | \$0.00     |
| <b>18b(1). Travel and Per Diem to Non-Federal Members</b>             | \$0.00        | \$0.00     |
| <b>18b(2). Travel and Per Diem to Federal Members</b>                 | \$0.00        | \$0.00     |
| <b>18b(3). Travel and Per Diem to Federal Staff</b>                   | \$0.00        | \$0.00     |
| <b>18b(4). Travel and Per Diem to Non-member Consultants</b>          | \$0.00        | \$0.00     |
| <b>18c. Other(rents,user charges, graphics, printing, mail, etc.)</b> | \$0.00        | \$0.00     |
| <b>18d. Total</b>   | \$0.00        | \$0.00     |

**19. Federal Staff Support Years  
(FTE)**

0.00 0.00

**20a. How does the Committee accomplish its purpose?**

The Information Security and Privacy Advisory Board's (Board or Advisory Board) 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 are leaders and experts from private industries, academia, federal agency CIOs, IGs and CISOs. An annual report is submitted and can be viewed at NIST's Computer Security Resource Center (CSRC) webpage:

<https://csrc.nist.gov/Projects/ispab/documentation>.

**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 twelve members including Chairperson, and is currently in the process of vetting one new member.

**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, the Board reviews and updates its work plan items for fiscal year. Topics include NIST publications and guidance, Activities/Challenges/Planning for Executive Orders, and Resources for National Cybersecurity Strategy, Post Quantum Encryption and Cryptographic Transitions, Software Bill of Materials (SBOM), Artificial Intelligence, NIST Cybersecurity and Privacy Frameworks, and Cybersecurity Workforce.

**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**

During this fiscal year, the board submitted three recommendation letters to CISA, DHS, and NIST, related to Software Bill of Materials (SBOM) and has one additional recommendation to CISA in draft. Recommendations and subsequent responses received can be viewed at: <https://csrc.nist.gov/Projects/ispab/documentation>.

**Designated Federal Officer**

Jeff Brewer DFO

| Committee Members | Start      | End        | Occupation  | Member Designation                       |
|-------------------|------------|------------|---|--|
| Baker, Brett      | 03/15/2022 | 03/14/2026 | Inspector General for the National Archives, National Archives and Records Administration | Regular Government Employee (RGE) Member |

|                              |            |            |  |  |
|------------------------------|------------|------------|--|--|
| Duffy, Michael               | 03/14/2024 | 03/13/2028 | Associate<br>Director for<br>Capacity,<br>Cybersecurity<br>Division,<br>CISA, DHS                        | Regular<br>Government<br>Employee<br>(RGE)<br>Member |
| Fanti, Giulia                | 07/09/2021 | 07/08/2025 | Assistant<br>Professor,<br>Carnegie<br>Mellon<br>University  | Special<br>Government<br>Employee<br>(SGE)<br>Member |
| Fitzgerald-McKay,<br>Jessica | 12/11/2020 | 03/03/2027 | Co-Lead,<br>Center for<br>Cyber<br>Security<br>Standards,<br>NSA   | Regular<br>Government<br>Employee<br>(RGE)<br>Member |
| Gantman, Alex                | 12/21/2022 | 12/20/2026 | Vice<br>President,<br>Security<br>Engineering:<br>Head of<br>Product<br>Security,<br>Qualcomm            | Special<br>Government<br>Employee<br>(SGE)<br>Member |
| Gattoni, Brian               | 08/07/2023 | 08/06/2027 | Department of<br>Homeland<br>Security  | Regular<br>Government<br>Employee<br>(RGE)<br>Member |
| Goodwin, Cristin             | 05/09/2022 | 05/19/2026 | Founder,<br>Advancing<br>Cyber   | Special<br>Government<br>Employee<br>(SGE)<br>Member |
| Groman, Marc                 | 09/12/2021 | 09/11/2025 | Principal,<br>Groman<br>Consulting,<br>Adjunct<br>Professor at<br>Georgetown<br>University Law<br>Center | Special<br>Government<br>Employee<br>(SGE)<br>Member |
| Hallawell, Arabella          | 01/26/2020 | 01/25/2024 | Executive<br>Vice President<br>- Marketing,<br>WhiteSource   | Special<br>Government<br>Employee<br>(SGE)<br>Member |
| Lipner, Steven               | 05/31/2018 | 05/30/2026 | Executive<br>Director,<br>Safecode   | Special<br>Government<br>Employee<br>(SGE)<br>Member |

|                   |            |            |  |  |
|-------------------|------------|------------|--|--|
| Miller, Essye     | 06/04/2021 | 06/03/2025 | President,<br>Executive<br>Business<br>Management            | Special<br>Government<br>Employee<br>(SGE)<br>Member |
| Moussouris, Katie | 07/09/2021 | 07/08/2025 | CEO, Luta<br>Security  | Special<br>Government<br>Employee<br>(SGE)<br>Member |
| Venables, Philip  | 03/05/2024 | 03/04/2028 | Chief<br>Information<br>Security<br>Officer,<br>Google Cloud | Special<br>Government<br>Employee<br>(SGE)<br>Member |

**Number of Committee Members Listed: 13**

### Narrative Description

The Board advises 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                  | <input type="checkbox"/>            |
| Trust in government                               | <input checked="" type="checkbox"/> |
| Major policy changes                              | <input type="checkbox"/>            |
| Advance in scientific research                    | <input checked="" type="checkbox"/> |
| Effective grant making                            | <input type="checkbox"/>            |
| Improved service delivery                         | <input checked="" type="checkbox"/> |
| Increased customer satisfaction                   | <input checked="" type="checkbox"/> |
| Implementation of laws or regulatory requirements | <input type="checkbox"/>            |
| Other   | <input type="checkbox"/>            |

### Outcome Comments

NA

**What are the cost savings associated with this committee?**

Checked if Applies

|                            |                                     |
|----------------------------|-------------------------------------|
| None                       | <input type="checkbox"/>            |
| Unable to Determine        | <input checked="" type="checkbox"/> |
| Under \$100,000            | <input type="checkbox"/>            |
| \$100,000 - \$500,000      | <input type="checkbox"/>            |
| \$500,001 - \$1,000,000    | <input type="checkbox"/>            |
| \$1,000,001 - \$5,000,000  | <input type="checkbox"/>            |
| \$5,000,001 - \$10,000,000 | <input type="checkbox"/>            |
| Over \$10,000,000          | <input type="checkbox"/>            |
| Cost Savings Other         | <input type="checkbox"/>            |

**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?**

52

**Number of Recommendations Comments**

For fiscal year 2023, the Board submitted a total of 3 recommendations.

**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: through email to the DFO and members; formal statements during the public opening session in meetings; or the dedicated ISPAB website.

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

Checked if Applies

|                                   |                                     |
|-----------------------------------|-------------------------------------|
| Reorganized Priorities            | <input checked="" type="checkbox"/> |
| Reallocated resources             | <input checked="" type="checkbox"/> |
| Issued new regulation             | <input type="checkbox"/>            |
| Proposed legislation              | <input type="checkbox"/>            |
| Approved grants or other payments | <input type="checkbox"/>            |
| Other                             | <input checked="" type="checkbox"/> |

## **Action Comments**

NIST continues to refine 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               | <input checked="" type="checkbox"/> |
| Online Agency Web Site    | <input checked="" type="checkbox"/> |
| Online Committee Web Site | <input checked="" type="checkbox"/> |
| Online GSA FACA Web Site  | <input checked="" type="checkbox"/> |

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.