2022 Annual Report

Information Security and Privacy Advisory Board

ISPAB

National Institute of Standards and Technology

U.S. Department of Commerce

Preface

The Information Security and Privacy Advisory Board (ISPAB or Board) was established in January 1988, as Congress enacted the Computer Security Act of 1987 (Public Law 100-235), which established the Board, and in accordance with the E-Government Act (Public Law 107-347), Title III, the Federal Information Security Management Act of 2002, amended the charter authority of the Board to its present form. The Information Security and Privacy Advisory Board is authorized by 15 U.S.C. § 278g-4, as amended. The ISPAB is a Federal Advisory Committee Act (FACA) committee, and it advises NIST, the Secretary of the Department of Homeland Security (DHS), and the Director of the Office of Management and Budget (OMB) on information security and privacy for federal government systems, including through review of proposed standards and guidelines developed by the National Institute of Standards and Technology (NIST). The Board's authority does not extend to private sector or federal systems which process classified information.

NIST values the diverse and highly respected perspectives from the ISPAB members and the Board's sound advice on NIST and the Federal Government strategic direction, programs, and operations. The function of this Committee cannot be performed by any other existing committee within the Department of Commerce (DOC) or the Federal Government.

Additional information regarding the ISPAB, such as membership, meetings, ISPAB's work plan, and documentation can be found at NIST's Computer Security Resource Center (CSRC) website: https://csrc.nist.gov/projects/ispab, as well as at the Federal Advisory Committee Act (FACA) Database: https://www.facadatabase.gov/FACA/FACAPublicPage.

This 2022 Annual Report covers the period from the beginning of October 2021 through September 2022 (Fiscal Year 2022).

ISPAB Members During this Annual Report

Steven Lipner, Chair
Executive Director
SAFECode
Term: 05/31/22 – 05/30/26

Dr. Brett Baker
Inspector General for the National Archives
U.S. National Archives & Records Administration
Term: 03/15/2022 – 03/14/2026

Ms. Giulia Fanti
Assistant Professor
Carnegie Mellon University
Term: 07/09/2021 – 07/08/2025

Ms. Jessica Fitzgerald-McKay
Co-Lead, Center for Cyber Security Standards
National Security Agency
Term: 12/11/2020 – 03/03/2023

Mr. Brian Gatton
Chief Technology Officer, (CISA)
Department of Homeland Security
Term: 08/07/19 – 08/06/23

Ms. Cristin Goodwin
General Manager & Associate General Counsel
Microsoft
Term: 05/09/2022 – 05/08/2026

Mr. Marc Groman
Principal, Groman Consulting Group LLC
& Adjunct Professor, Georgetown Law
Term: 09/12/2021 – 09/11/2025

Ms. Arabella Hallawell
Executive Vice President
WhiteSource
Term: 01/26/2020 – 01/25/2024

Mr. Douglas Maughan
Head of Office of Convergence Accelerators
National Science Foundation
Term: 08/07/2019 -08/06/2023

Ms. Essye Miller
President
Executive Business Management
Term: 06/04/2021 – 06/03/2025

Ms. Katie Moussouris
CEO & Founder
Luta Security
Term: 07/09/2021 – 07/08/2025

Mr. Philip Venables
Chief Information Security Officer
Google Cloud
Term: 03/05/2020 – 03/04/2024

ISPAB Secretariat
Mr. Matthew Scholl
Chief, Computer Security Division
National Institute of Standards & Technology

ISPAB Designated Federal Officer
Mr. Jeff Brewer
Management & Program Analyst
National Institute of Standards & Technology

Table of Contents

ISPAB Focus for Fiscal Year 2022

Topic 1: Executive Order 14028, Improving the Nation's Cybersecurity,

Topic 2: NIST Publications and Guidance (Cybersecurity and Privacy),

Topic 3: Cryptography and Quantum Computing,

Topic 4: Bug Bounties, Advanced Persistent Threats, and Vulnerability Disclosures,

Topic 5: Artificial Intelligence and Supply Chain Issues.

ISPAB Meeting Information for Fiscal Year 2022

1) Information Security and Privacy Advisory Board (ISPAB) December 2021 Meeting

Date: December 08 - 09, 2021
Location: Virtual Via Blue Jeans
Open to the public

Presentations and/or Briefings:

- DHS – Executive Order (EO) 14028: DHS Incident Response Playbook,
- GSA – EO 14028 Section – FedRAMP Updates,
- NIST - Cybersecurity and Privacy Updates,
- NIST – Crypto Agility Project at NCCoE,
- NIST – EO 14028 Software Security Development Framework,
- NIST - Information Technology Laboratory Overview and Updates,
- NIST- Privacy Program Update,
- NIST – Update to FIPS 201 and Identity Mechanisms.

More information such as the Federal Register Notice, full agenda, and related detailed Meeting Minutes can be found at ISPAB's event page: https://csrc.nist.gov/Events/2021/ispab-december-2021-meeting

Recommendations from this Meeting

Recommendation on Executive Order (EO) 14028 "Improving the Nation's Cybersecurity"
ISPAB submitted a letter to NIST, DHS, and OMB expressing concern about the magnitude of effort that the EO will require from government agencies and private sector along with the inquiry regarding implementation guidance.

Letter to Dr. James Olthoff, Performing the Non-Exclusive Functions and Duties of the Undersecretary of Commerce for Standards and Technology and Director, NIST, the Honorable Alejandro Mayorkas, Secretary, United States Department of Homeland Security, and Ms. Shalanda D. Young, Acting Director, Office of Management and Budget.

2) Information Security and Privacy Advisory Board (ISPAB) March 2022 Meeting

Date: March 09 - 10, 2022
Location: Virtual via Blue Jeans
Open to the public

Presentations and/or Briefings:

- Academy Panel – National Academy of Public Administration Report: A Call to Action: The Federal Government's Role in Building a Cybersecurity Workforce for the Nation,
- CISA (DHS) – GovCAR Overview and Use,
- Congressional Research Service – Congressional Research Service Report (R46926) on Federal Cybersecurity: Background and Issues for Congress,
- GAO – GAO Report: Federal Response to SolarWinds,
- NIST – Cybersecurity and Privacy Update,
- NIST – Information Technology Laboratory Overview and Updates,
- NIST – Open Security Controls Assessment Language (OSCAL),
- NSA – National Security Council Efforts on Open-Source Software Security,
- ONCD – Office of the National Cyber Director Introduction and Update,
- Public Comments and Board Discussion,
- Senate Committee on Commerce, Science, and Transportation – Senate Commerce Priorities in Cybersecurity.

More information such as the Federal Register Notice, full agenda, and related detailed Meeting Minutes can be found at ISPAB's event page: https://csrc.nist.gov/Events/2022/ispab-march-2022-meeting.

Recommendations from this Meeting

None

3) Information Security and Privacy Advisory Board (ISPAB) July 2022 Meeting

Date: July 13 – 14, 2022
Location: Hybrid (In-Person and Virtual using Blue Jeans)
Open to the public

Presentations and/or Briefings:

- DHS – DHS Binding Operational Directive (BOD) 22-01 – Develop and Publish A Vulnerability Disclosure Policy, and the Known Exploitable Vulnerabilities List,
- FTC – Federal Trade Commission Patching Guidance,
- Forescout – Threat Briefing – Current Advanced Persistent Threats (APT) Activities,
- NIST – Artificial Intelligence (AI) Security Metrics and Threats,
- NIST – Cybersecurity and Privacy Update,
- NIST – Information Technology Laboratory Overview and Updates,
- NIST & CISA (DHS) – National Security Memo on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10),
- NIST – Security of Hardware,
- NIST – Supply Chain Risk Management – National Initiative for Improving Cybersecurity in Supply Chains,
- NIST – Updates to the Cybersecurity Framework,
- MITRE – MITRE ATT&CK Framework,
- Public Comments and Board Discussions,

More information such as the Federal Register Notice, full agenda, and related detailed Meeting Minutes can be found at ISPAB's event page: https://csrc.nist.gov/Events/2022/ispab-july-2022-meeting.

Recommendations from this Meeting

None

ISPAB Charter

The current ISPAB Charter was renewed in February 2022 and information can be found at ISPAB's event page: https://csrc.nist.gov/projects/ispab. The current charter expires February 23, 2024.

ISPAB Meeting Costs for Fiscal Year 2022

Category	Estimated Costs	Actual Costs
Payments to Non-Federal Members	$0	$0
Payments to Federal Members	$16,000	$15,691
Payments to Federal Staff	$50,000	$42,026
Payments to Consultants	$0	$0
Reimbursement for Travel: Non-Federal Members	$10,000	$4,555
Reimbursement for Travel: Federal Members	$800	$0
Reimbursement for Travel: Federal Staff	$1,000	$81
Reimbursement for Travel: Consultants	$0	$0
Other Costs	$50,000	$49,979
Federal Staff Support:	.50	.30
Total	$127,800	$112,332

Questions or comments regarding this annual report can be directed to ISPAB's Designated Federal Officer (DFO) – Jeff Brewer (Jeffrey.Brewer@nist.gov).