

Privacy Controls Workshop: Next Steps for NIST Special Publication 800-53, Appendix J

September 8, 2016
Washington, DC

(Updated: Sept. 7, 2016)

This workshop is co-hosted by the National Institute of Standards and Technology (NIST) and the Department of Transportation (DOT) to gather input on the privacy controls in Appendix J of NIST Special Publication 800-53, Revision 4. The goal is to explore the effectiveness and challenges of applying the current privacy controls in 800-53 and what changes should be made in the publication's fifth revision.

9:00 Opening Remarks

Kevin Stine, Chief, Applied Cybersecurity Division, NIST

Claire Barrett, Chief Privacy Officer, DOT

Marc Groman, Senior Advisor for Privacy, Office of the Director, OMB

9:20 Panel Discussion

This panel will provide background and considerations for the breakout discussions to follow. Panelists will cover how security controls were developed and their relationship to information security risk management, operational benefits and challenges with Appendix J today; and new considerations around privacy risk management and the role of privacy controls in the building of more effective privacy programs.

Sean Brooks, Privacy Engineer, NIST

*Jamie Danker, Senior Privacy Officer, National Protection &
Programs Directorate, DHS*

Naomi Lefkowitz (Moderator), Senior Privacy Policy Advisor, NIST

Ron Ross, Fellow, NIST

Stuart Shapiro, Principal Cyber Security and Privacy Engineer, MITRE

10:20 Break

10:30 Breakout Session (Check your badge for room number)

Topics of discussion for this session will include benefits and challenges of Appendix J and basic restructuring such as overlapping controls, improved categorization of privacy controls; and the use of control enhancements and supplemental guidance to provide more privacy considerations

12:00 Lunch (on your own)

1:00 Breakout Session (Check your badge for room number)

Topics of discussion for this session will include privacy frameworks that will support improved assessment of privacy controls; new controls or control families to improve privacy risk management; and a final review of proposed changes for effectiveness or disadvantages.

2:45 Closing Remarks and Next Steps

Naomi Lefkowitz, Senior Privacy Policy Advisor, NIST

3:00 Adjourn

Privacy Controls Workshop: Next Steps for NIST Special Publication 800-53, Appendix J

September 8, 2016
Washington, DC

Meet the Speakers

Claire Barrett has over 20 years of experience working in the field of privacy and data protection. She has served as the Chief Privacy and Information Asset Officer at the US Department of Transportation since 2011. In that capacity she is responsible for a broad range of programs addressing the Department's collection, use, and maintenance of information. Her portfolio include Privacy Risk Management, Records Management, Paperwork Reduction Act, and IT Policy. In addition to ensuring that the Department remains compliant with information management requirements Ms. Barrett works to promote inter and intra-program relationships so that the Department's information and data practices bring the greatest value to the Department while ensuring protection of individual privacy. Prior to joining the USDOT, Ms. Barrett was a component privacy officer with the Department of Homeland Security and served as a consultant to private and public sector clients addressing privacy and cybersecurity needs. Ms. Barrett holds a BA from James Madison University in International Policy and nearing completion of her MA at Mercyhurst University. Outside of the office Claire is an active member of Toastmasters International and spends weekends with her husband trying to teach their two beagles not to dig massive holes in the backyard looking for lost bones.

Sean Brooks represents the Applied Cybersecurity Division of the National Institute of Standards and Technology (NIST) on the west coast. He supports a broad range of NIST projects, including the National Strategy for Trusted Identities in Cyberspace program office and the new privacy engineering program. Previously, he worked in the San Francisco office of the Center for Democracy and Technology, a non-profit public interest organization focused on civil liberties and human rights issues online. Sean has also supported Silicon Valley companies ranging from multinational information security and business intelligence companies to consumer technology start-ups. Sean received his MPA at NYU's Wagner Graduate School of Public Service, where he was a graduate research fellow with The Governance Lab and the NYU Center for Interdisciplinary Studies in Security and Privacy. He received his undergraduate degree in politics from the University of California at Santa Cruz.



Jamie Danker is the Director, Senior Privacy Officer, DHS National Programs and Protection Directorate and leads the DHS National Programs and Protection Directorate Privacy Program where she and her team support and advocate for building privacy into the earliest stages of program and system development. Danker has held various privacy positions within DHS, including at the DHS Privacy Office where she developed and implemented the Privacy Compliance Review Framework. She also served as the Privacy Officer for the U.S. Citizenship and Immigration Services Verification Division's E-Verify and related programs. Prior to joining DHS, Danker led and contributed to a number audits concerning government-wide and agency-specific privacy issues at the U.S. Government Accountability Office.



Privacy Controls Workshop: Next Steps for NIST Special Publication 800-53, Appendix J

September 8, 2016
Washington, DC

Marc Groman, as the Senior Advisor for Privacy, reports directly to OMB Director Shaun Donovan and is the principal advisor for privacy policy issues in the Federal Government. Marc is responsible for developing and implementing government-wide strategies ensuring department and agency compliance with privacy requirements. He serves as the Federal Government representative on privacy policy matters in both domestic and international forums. In addition, he works with the Federal CIO and CTO to ensure that adequate privacy protections are included in all new major Federal IT projects. Marc coordinates with other policy offices across the Executive Office of the President to develop and administer the Administration's privacy policy. Marc also serves as the Chairman of the Federal Privacy Council which was established by President Obama in February 2016. Prior to joining OMB, Marc served as the President and Chief Executive Officer of the Network Advertising Initiative, a technology trade association representing members such as Google, Microsoft, Facebook and AOL.



Naomi Lefkovitz has served as Senior Privacy Policy Advisor at NIST since March 2012, specializing in the impact on privacy from digital identity management, cybersecurity and other information technologies. Lefkovitz previously served as Director for Privacy and Civil Liberties, Cybersecurity Directorate in the White House and Senior Attorney, Division of Privacy and Identity Protection in the Federal Trade Commission, where her specialty areas included online privacy, digital identity management, data security and consumer financial protection laws.



Ron Ross is a Fellow at the National Institute of Standards and Technology (NIST). His current focus areas include information security and risk management. Dr. Ross leads the Federal Information Security Modernization Act (FISMA) Implementation Project, which includes the development of security standards and guidelines for the federal government, contractors, and the United States critical infrastructure. He also is the principal architect of the Risk Management Framework (RMF), a multi-tiered approach that provides a disciplined and structured methodology for integrating the suite of FISMA-related standards and guidelines into a comprehensive enterprise-wide security program. In addition to this work, Dr. Ross leads the Joint Task Force, an interagency partnership with the Department of Defense, the Office of the Director National Intelligence, the U.S. Intelligence Community, and the Committee on National Security Systems (CNSS) that developed the Unified Information Security Framework for the federal government and its contractors. Dr. Ross previously served as the Director of the National Information Assurance Partnership, a joint activity of NIST and the National Security Agency.



Privacy Controls Workshop: Next Steps for NIST Special Publication 800-53, Appendix J

September 8, 2016
Washington, DC

Stuart S. Shapiro is a Principal Cyber Security and Privacy Engineer at the MITRE Corporation, a not-for-profit company operating federally funded research and development centers (FFRDCs). At MITRE he has led multiple research and operational efforts in the areas of privacy engineering, privacy risk management, and privacy enhancing technologies (PETs) and has written and presented on these in numerous forums. Among his professional affiliations are the International Association of Privacy Professionals (IAPP), the Advisory Board of the Ponemon Institute's Responsible Information Management Council, and the US Public Policy Council of the Association for Computing Machinery (USACM) where he currently serves as Chair.



Kevin Stine is the Chief of the Applied Cybersecurity Division in the National Institute of Standards and Technology's Information Technology Laboratory. In this capacity, he leads NIST collaborations with industry, academia, and government on the practical implementation of cybersecurity and privacy through outreach and effective application of standards and best practices. The Applied Cybersecurity Division develops cybersecurity and privacy guidelines, tools, and reference architectures in diverse areas such as public safety communications; health information technology; smart grid, cyber physical, and industrial control systems; and programs focused on outreach to small businesses and federal agencies.



The Division is home to several priority national programs including the National Cybersecurity Center of Excellence, the National Strategy for Trusted Identities in Cyberspace, and the National Initiative for Cybersecurity Education (NICE). Recently, he led NIST's efforts to develop the Framework for Reducing Cybersecurity Risk to Critical Infrastructure (Cybersecurity Framework) as directed in Executive Order 13636.