Assessing Privacy Controls Workshop Summary

Privacy Practitioners Seek Guidance and Collaboration

On May 18th, NIST's Privacy Engineering Program hosted the Assessing Privacy Controls Workshop in Gaithersburg, Maryland, as part of an ongoing series of workshops on privacy engineering and risk management. At the workshop, stakeholders provided feedback on incorporating privacy, for the first time, into the upcoming fifth revision of NIST Special Publication (SP) 800-53A, Assessing Security and Privacy Controls in Federal Information Systems. They also shared current procedures for assessing privacy controls, along with their challenges and lessons learned. With over 150 in-person attendees and 225 attendees online for the opening session, the workshop proved to be a valuable opportunity for collective education.

Opening Up the Discussion

The morning began with opening remarks from Kevin Stine, Chief of the NIST Applied Cybersecurity Division, and Naomi Lefkovitz, NIST Senior Privacy Policy Advisor, emphasizing the value NIST receives from stakeholder input and the importance of integrating privacy into NIST risk management publications. Ellen Nadeau, NIST Privacy Risk Strategist, then moderated a panel featuring Claire Barrett, Chief Privacy Officer at the U.S. Department of Transportation; Victoria Pillitteri, NIST Advisor for Information System Security; and Lindsay Lennon Vogel, Senior Director, Privacy Compliance, Privacy Office, U.S. Department of Homeland Security. Victoria Pillitteri provided insights on approaches to controls assessment, updates on SP 800-53A and other NIST SPs, and Federal Information Security Management Act (FISMA) perspectives, Claire Barrett and Lindsay Lennon Vogel shared operational privacy experiences and insights from their agencies.

Key takeaways from panelists included:

- **Privacy is too often brought into the risk management process later, as a compliance exercise**, as opposed to building privacy considerations in at the design phase of a system's lifecycle. Privacy and security teams need to collaborate sooner and in a manner that is proactive rather than reactive.
- There are many **potential benefits of collaboration between security and privacy practitioners**, including enabling privacy teams to leverage security test results (and vice versa), and to participate early in the enterprise risk management process, including business discussions.
- Although privacy-security collaboration is built into the starting steps of the latest draft revision of NIST SP 800-37, **there will likely be initial growing pains in combining processes that previously ran as two parallel tracks**.

If you were unable to attend the workshop, a video recording of the first hour of the event is available on NIST's event page.

Diving into Privacy Control Assessments

The workshop featured four facilitated breakout rooms for open, but non-attributable discussion on conducting privacy control assessments, and where to focus guidance based on experiences in both the federal and commercial spaces. In these breakouts, participants discussed how they are currently assessing privacy controls, what challenges they face, and how assessment practices can be improved. Participants also discussed privacy control assessors' typical skillsets, how they collaborate with their

security counterparts, and how automation might be used to enhance the privacy control assessment process.

A number of themes emerged from the breakout rooms, including:

- **Beyond compliance:** Many participants were interested in moving privacy controls assessments beyond "check the box" compliance exercises—such as simply confirming a privacy document, like a System of Records Notice (SORN), exists—and instead would like to more thoroughly analyze the effectiveness of privacy controls.
- **Security and privacy teams' collaboration:** There is still progress to be made in building relationships between security and privacy professionals to work together more effectively. The size and strength of privacy teams across organizations varies widely, but is often secondary in size and priority to security, according to workshop attendees.
- **SDLC engagement:** Participants expressed that privacy needs to be involved from the beginning of, and throughout, the system development life cycle to avoid surprises and roadblocks once the authority to operate stage is reached. Many participants hoped that NIST guidance would help facilitate this earlier involvement and improve communication between privacy and security domains and across the organization as a whole. This NIST guidance not only includes SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*—but also updated versions of SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*, and SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.
- **Assessor skills and training:** Participants called out backgrounds in privacy, risk management, IT audit, and legal as some important skillsets of a privacy assessor. They also highlighted the need for training, both to bolster the strengths of existing privacy professionals and also when security control assessors are conducting the assessments, to teach them what to look for. It was noted that security and privacy teams often seem to be speaking two different languages.
- **Automation:** Automation of privacy control assessments is a material gap area in many organizations. Though organizations aspire to perform continuous monitoring for privacy, the participants noted barriers, such as a lack of: resources, adequate privacy integration with existing security information and event monitoring tools, and appropriate solutions in the market. Nevertheless, many participants conveyed that automation is key to making privacy control implementations more effective and consistent. Some participants hoped that the integration of privacy into 800-53A would enable the development of more automated tools.

Next Steps

NIST will use the feedback from the workshop as it begins to integrate privacy into 800-53A. Use the online schedule for NIST FISMA publications to keep updated on any changes.

If you would still like to provide input on this topic, NIST welcomes written feedback at PrivacyEng@nist.gov on the workshop's supplemental resources.

To stay in the loop on future updates and events, sign up for email updates from the NIST Privacy Engineering Program here and follow @NISTcyber. To learn more about NIST's Privacy Engineering Program, visit the program's website.