NIST Risk Management Framework Workshop Summary
October 3, 2017
National Cybersecurity Center of Excellence

The National Institute of Standards and Technology (NIST) convened users of the NIST Risk Management Framework (RMF) to discuss how it is currently being used by stakeholders in the private sector and across the federal government, successes and challenges with its use, and opportunities for enhancement through simplification, innovation, and automation. In anticipation of this workshop, NIST released a discussion draft of SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A Systems Life Cycle Approach for Security and Privacy. The half-day workshop was held at the National Cybersecurity Center of Excellence, the first Federally Funded Research and Development Center where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. Dr. Charles Romine, Director of the Information Technology Laboratory (ITL), provided welcoming remarks, an overview of the breadth of ITL's research portfolio, and thanked stakeholders for their ongoing engagement.

The first workshop speakers gave a **Policy Update from the Office of Management and Budget** (OMB). Ross Nodurft, OMB Cyber Unit Chief, provided an update on the Report to the President on Federal IT Modernization, and the government-wide risk report that was also recently submitted. These efforts in response to Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, highlight the importance of collaboration in the implementing risk management for systems and the opportunity to enhance the agility of security in federal networks. Taylor Roberts, Cybersecurity Policy Analyst in OMB Cyber, provided an update on recent efforts by an interagency working group formed by the Federal CIO and CISO councils to provide input into the RMF and NIST Special Publication 800-53, Rev. 5 Initial Public Draft control baselines. Finally, Charles Cutshall, Senior Policy Analyst at the Office of Information and Regulatory Affairs, OMB, discussed the integration of privacy into both the RMF and SP 800-53 controls to parallel the efforts of privacy integration in OMB Circular A-130.

The second session at the workshop featured an **Update on the NIST Risk Management Framework and the Cybersecurity Framework**. Ron Ross, NIST Fellow, gave an overview of the key drivers to the updates of the RMF and SP 800-53, and an overview of the major updates to each publication. Significant updates to the RMF (for additional information, see the Discussion Draft of SP 800-37, Rev. 2) includes:

- Closer linkage and communication processes/activities at the C-suite level of the organization and the processes and activities at the system and operational level of the organization through the Organizational Preparation Step;
- How the Cybersecurity Framework can be implemented using established risk management practices (e.g., developing a Federal use case); and
- An integration of privacy concepts into the RMF.

These updates intend to facilitate better communication between senior leaders and missions/business process and system owners; encourage organization-wide identification of common controls and tailored control baselines (to reduce the burden of selecting and implementing controls on systems); and identify, prioritize and focus efforts on high-value assets and systems. Naomi Lefkovitz, Senior Privacy Advisor at NIST, discussed the privacy integration process for both controls in SP 800-53 and the RMF methodology. Matt Barrett, Cybersecurity Framework Program Manager at NIST, shared updates on the Cybersecurity Framework and Draft NISTIR 8170.

The panel, **Automation Tools for Risk Management**, moderated by Kevin Cox, Continuous Diagnostics and Mitigation (CDM) Program Manager at the Department of Homeland Security, highlighted ongoing federal efforts to identify and leverage automation tools used in industry for federal risk management, the recent GSA Request for Information on ATO Automation Tools, and representatives from two automation tool vendors. Matt Goodrich, Director of the FedRAMP Program, has been working with the Office of American Innovation to reduce the time for a system to get through the FedRAMP process, with a focus on increasing the use of automation. To that end, the General Services Administration (GSA) released a Request for Information on Authority To Operate (ATO) Automation Tools to identify existing tools and products available to help automate the RMF process for one or more steps of the RMF. Aiden Feldman, Project Boise Team Lead at GSA discussed current efforts to evaluate the ATO landscape and determine where GSA can provide the most value and assist federal agencies, and discussed next steps for the project team. The two industry representatives, Daniel McGregor, Senior Systems Engineer at Vitustream and Cary Riddock, Senior Director and BlueCanopy, discussed their products' capabilities as examples of automation tools currently available that provide the asset management, and accelerate and automate the RMF process, including providing overlays of applicable SP 800-53 controls. In addition to highlighting current federal efforts and available tools, panel discussion covered future needs that additional resources could provide, including: a repository to share ATO documentation, interoperability of automation tools, and their data sets, and a forum to disseminate and share best practices.

Following the panel, the Department of Justice, Office of the Chief Information Officer, shared a **demonstration of the Cyber Security Assessment and Management (CSAM) Version 4.0 too**l, featuring key functionality updates in the Portal, Security Posture Dashboard Report (SPDR) scoring and integration, and control assessment risk scoring. CSAM v 4.0 provides a portal/platform of capabilities, services and tools to support a federal agency's cybersecurity mission and objectives. CSAM is an example of a federal tool available to help with ATO Automation that provides a risk scoring methodology at the organization, system, and control level.

The panel, **Industry Approaches to Risk Management in the Systems Development Lifecycle (SDLC)**, featured private sector organizations and how their organizations manage risks as they design, build, maintain, and retire systems, current industry best practices and lessons learned that can help federal agencies. Panelists included Matt Coose, CEO of Qmulos, Steve Horvath, Vice President of Strategy and Vision at Telos, and John McClurg, Vice President and

Ambassador-at-Large of Cylance. All three organizations primarily use an Agile development process to develop the products they deliver to customers and followed similar best practices for risk management. For example, panelists highlighted the importance of code reviews, regression testing, and implementing continuous monitoring. However, each organization leveraged different standards and guidelines, including RMF, OWASP, SP 800-171, among others. A common theme in the discussion of best practice and lessons learned included the value of simplicity, inheriting security controls, increased automation where feasible, and ongoing stakeholder engagement and buy-in. Panelists agreed that the misguided approach of "check-the-box" compliance for security is insufficient, but there is no easy solution to solve this complex challenge that includes a need for metrics, continuous monitoring, threat modeling and more.

The final speaker, Eric Mill, Senior Advisor at the Technology Transformation Service at GSA, presented on Balancing Security and Efficiency in System Development, and proposed alternative approaches for risk management. This presentation highlighted some common challenges faced by federal agencies in terms of implementing security, including a lack of efficiency and criticism of the current SP 800-53 control baselines and how they are implemented. To address these challenges, Eric proposed four organizing principles and alternative approaches:

1. Focus on important (e.g., high-value and high impact) systems and their protection. Eric encouraged the use of an alternative threat-based control selection and issuance of ATOs, and refocusing our efforts away from securing low impact systems (more effort on high-value and high impact systems) to get systems into production faster;
2. Empirical evidence over documentation. He encouraged the use of public vulnerability disclosure and bug bounties, as well as Increased peer review, especially in contracted software development.
3. Agility is security. There is the opportunity to focus on metrics, shorten patch time, and increase the use of automated test suites.
4. Reducing risk of the status quo. By redirecting time and money to the right place, using better metrics, there is the opportunity to improve how risk management is currently implemented.

However, Eric acknowledged that there is not a single alternative or framework to address this issue.

The workshop concluded with an open discussion facilitated by NIST on the Discussion Draft of SP 800-37 and next steps. Questions included requests for updates to additional NIST Special Publications such as SP 800-18, FIPS 200, SP 800-47 and SP 800-60. The NIST team is currently adjudicating comments on the Initial Public Draft of SP 800-53, Revision 5 and anticipates releasing a second public draft in Winter 2017. An initial public draft of SP 800-37 will also be released in the Winter of 2017.