MITRE Center for Data-Driven Policy

EIGHT RECOMMENDATIONS FOR CONGRESS TO IMPROVE FEDERAL CYBERSECURITY

By Mark Peters, Dave Powner, and Chris Folk

Eight recommendations for Congressional action to improve federal agency cybersecurity while increasing the efficiency and effectiveness of its oversight efforts

1. **Give Federal Cybersecurity Leadership More Authority to Oversee Cyber Risk Management at Agencies and Departments.** Strengthen the National Cyber Director, Federal CIO, and Federal CISO offices so that they have the capacity and authority to actively help agencies prioritize, act on, and measure progress to create greater unity of effort across government.
2. **Identify and Modernize Complex Legacy IT Systems to Reduce Costs and Vulnerabilities.** Identify and modernize those mission-critical systems that contribute most to maintenance costs and security vulnerabilities.
3. **Create an Integrated Cyber Risk Management Framework.** Create an approach to risk management that incorporates threat evaluation along with human and physical risk management.
4. **Support Zero Trust Architecture (ZTA) Implementation.** Ensure agencies have the resources needed to implement the plans developed under Executive Order 14028, and conduct oversight activities to monitor implementation efforts.
5. **Support Modernization of CISA Cyber Defense Systems.** Fund modernization of the National Cybersecurity Protection System (including EINSTEIN), the Continuous Diagnostics and Mitigation Program, and related services to help ensure CISA's ability to provide cyber defense and threat hunting as agencies move to cloud services and ZTA.
6. **Mandate Supply Chain Risk Management Assessments Throughout Program Lifecycles.** The Federal Acquisition Security Council, CISA, and NIST should transform supply chain risk assessments so that they operate throughout the lifecycle of programs.
7. **Update Congressional Oversight Using FITARA as a Model.** Replace long narrative agency reports with a model utilizing clear and concise priorities and measurable milestones of progress in a format conducive to Congressional oversight.
8. **Require That Cybersecurity Be a Cross-Agency Priority in the President's Management Agenda.** Ensure that cybersecurity is a key performance goal and shift toward use of metrics based on those used by CISOs and industry.

OCTOBER 2021

The Need for Further Congressional Action

It is time for additional Congressional action to help meet the changing threat landscape facing America today by updating law and policy regulating federal government cybersecurity, and by funding and overseeing modernization of federal IT and cybersecurity systems. Law governing federal agency cybersecurity and oversight last received a major update with passage of the Federal Information Security Modernization Act of 2014. Since then, the government has continued to struggle with both basic cybersecurity hygiene and advanced threats, as borne out by numerous reports from the Government Accountability Office (GAO) and agency inspectors general. Updates are needed to the laws governing federal cybersecurity to align them with current cybersecurity best practices, to reduce spending on audits and reports, and to clarify roles and responsibilities of the many federal players involved.

Further, federal agencies are taking action to modernize legacy IT systems and to update cybersecurity programs on their own initiative and with the leadership of the White House. Congress should weigh in with support for these efforts while also overseeing them on behalf of the public.

This paper identifies eight ways that Congress can act to improve federal cybersecurity practices and to meet the advanced threats posed by China, Russia, ransomware gangs, and other nation-state and criminal actors. These changes will improve the government's ability to deploy and maintain secure systems ready for today's threats and increase the effectiveness and efficiency of oversight activities.

Recommendations

1. Give Federal Cybersecurity Leadership More Authority to Oversee Cyber Risk Management at Agencies and Departments Authority over Executive Branch cybersecurity should be brought together into a more coordinated team structure with appropriate resources and staff to carry out their duties. The National Cyber Director's office and the Federal CIO and CISO offices need to be strengthened so that they are more than policy and oversight organizations, with capacity and authority to play an active role helping agencies prioritize and measure progress of their cyber efforts to create greater unity of effort across government.

2. Identify and Modernize Complex Legacy IT Systems to Reduce Costs and Vulnerability Congress and agencies should identify and modernize mission critical legacy systems that most contribute to agencies' maintenance costs and security vulnerabilities. Recent MITRE analysis shows that systems using many programming languages have disproportionately higher maintenance costs and security vulnerabilities. Identifying mission critical IT systems that use many programming languages is a way to help target modernization efforts toward systems most likely to generate disproportionate costs and exhibit greater security vulnerability.

3. Create an Integrated Cyber Risk Management Framework
Authorization and funding are needed to create a new and integrated threat-hunting-focused approach to cyber risk management. Existing cyber risk management techniques and tools have evolved over decades in a piecemeal fashion and have typically focused on managing vulnerabilities. Best practice in cybersecurity has shifted toward a threat-hunting focus, yet legacy risk evaluations retain a heavy focus on vulnerability management. It is time to take a comprehensive view that incorporates threat evaluation, along with human and physical risks,

to create an Integrated Cyber Risk Management Framework that identifies a holistic set of data relevant to measuring and managing cyber risks to organizations; provides analytical approaches to make effective use of this information to understand and score risks; and enables effective discussions among various stakeholders about risks and their mitigation.

4. Support Zero Trust Architecture (ZTA) Implementation

Congress should support agency implementation of ZTA principles by ensuring that agencies have the resources they need to implement their plans developed under Executive Order (EO) 14028 and by conducting oversight activities to monitor implementation efforts according to Administration guidance. To enable these actions, federal agencies should be tasked with reporting to Congress on their plans for and implementation of the concepts of trustless end points.

5. Support Modernization of CISA Cyber Defense Systems

Many of CISA's cyber defense systems were designed for an era when most agency systems were operated internally and most network traffic was unencrypted. In the years since, agencies have conducted extensive migrations of systems to cloud service providers and are beginning to implement ZTA for their networks. CISA has recognized this change and is seeking to update its suite of programs providing security services to federal agencies so that they provide effective defenses for today's agency IT architectures and better support threat-hunting activities by defenders. Congress can support these efforts by ensuring adequate funding for modernization of the National Cybersecurity Protection System (which includes the EINSTEIN system referenced in EO 14028), the Continuous Diagnostics and Mitigation Program, and other related efforts in the years ahead.

6. Mandate Supply Chain Risk Management Assessments Throughout Program Lifecycles

The SECURE Technology Act passed in 2018 established the interagency Federal Acquisition Security Council (FASC), which is chaired by the Federal CISO. The FASC has a broad mandate for both cyber and supply chain policy. In the past, supply chain risk assessments have been rare, and when performed are generally associated with final steps before a high-value acquisition. This approach does not address the ubiquitous, continuously evolving nature of supply chain risk. Continuous supply chain risk assessment and mitigation is essential to reducing incidents. The FASC, working with both CISA and NIST, needs to transform supply chain risk assessments so they operate from early-stage requirements definition through program lifecycle.

7. Update Congressional Oversight Using FITARA as a Model

Congress should update its oversight of agency cybersecurity by using the Federal Information Technology Acquisition Reform Act (FITARA) as a model to replace existing unstructured agency reporting. The FITARA scorecard provides transparency into key measures of agency progress in improving IT management every six months by establishing clear milestones against which all agencies measure and report their progress. Existing cybersecurity reporting requirements result in lengthy narratives subjectively describing agency cybersecurity programs, but not in concise and repeatable measurements of progress on key objectives across agencies. A FITARA-style cybersecurity scorecard can be the subject of Congressional oversight hearings where Executive Branch and agency leaders can testify on their progress and on areas where improvement and additional Congressional support is needed. This reporting model could also be used to streamline the extensive reporting agencies currently produce for

Congress, GAO, and the IG community. Because cybersecurity is a rapidly evolving field where both threats and defensive strategies change frequently, a more rapid reporting and oversight cycle would help Congress ensure that agencies are staying current with those changes and have the resources needed to do so.

8. Require That Cybersecurity Be a Cross-Agency Priority in the President's Management Agenda
Congress should require that cybersecurity be included as a specific Cross-Agency Priority (CAP) in the President's Management Agenda to ensure that cybersecurity is a key performance goal for the government each year. In implementing cybersecurity as a CAP, metrics should include measures comparable to how federal and business CISOs measure their organizations' performance and how cyber insurers evaluate client risk. These metrics can also be adopted in IG and GAO reviews to help ensure consistency across management and audit processes and to streamline the data collection process for agencies. More rapid completion of audits would help make audits a more actionable tool for management and oversight of federal cybersecurity.

Conclusion

Congress has taken many actions to support federal cybersecurity. However, cybersecurity is a rapidly evolving field and further action is needed to push federal cybersecurity forward. Congressional action can help ensure that the federal government is positioned to meet current and emerging threats and is managed according to current best practices. The eight recommendations in this paper provide options for Congress that would support efforts at improving federal agency cybersecurity while making the oversight process more efficient and effective.

About the Authors

Mark Peters is a cyber defense policy professional specializing in national preparedness for cyber incidents, with a special interest in integrating cyber incident response with broader emergency management processes. He joined MITRE in 2007 and has supported a variety of homeland and national security sponsors. In 2020 he was a Brookings LEGIS Congressional Fellow for Rep. Elissa Slotkin. He holds a bachelor's degree in computer engineering and a master's degree in computer science, both from Auburn University.

Dave Powner is the executive director for MITRE's Center for Data-Driven Policy. He previously led the Government Accountability Office's IT management, working closely with Congress, the Office of Management and Budget, and Federal Chief Information Officers on IT reform efforts including the Modernizing Government Technology Act, the FITARA, and the FITARA scorecard.

Chris Folk is MITRE's director for cybersecurity policy and strategic partnerships. He is responsible for facilitating policy guidance to complement technical solutions required to address challenges in securing the global cyber ecosystem. He has previously held positions with Amazon Web Services, the U.S. Navy, Department of Defense, Federal Bureau of Investigation, and Department of Energy. He holds a bachelor's degree from Saginaw Valley State University and a Master of Business Administration degree from Virginia Tech.

For information about MITRE's FISMA expertise and capabilities, contact Chris Folk, director for MITRE's Cybersecurity Policy and Strategic Partnerships, cjfolk@mitre.org or (703) 217-6329.

For more information about this paper or the Center for Data-Driven Policy, contact policy@mitre.org

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™