A REPORT OF THE CSIS TECHNOLOGY AND PUBLIC POLICY PROGRAM

Updating U.S. Federal Cybersecurity Policy and Guidance

SPENDING SCARCE TAXPAYER DOLLARS ON SECURITY PROGRAMS THAT WORK

Authors
Franklin S. Reeder
Daniel Chenok
Karen S. Evans
James A. Lewis
Alan Paller

October 2012

50 YEARS | CHARTING OUR FUTURE

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A REPORT OF THE CSIS
TECHNOLOGY AND PUBLIC
POLICY PROGRAM

Updating U.S. Federal Cybersecurity Policy and Guidance

SPENDING SCARCE TAXPAYER DOLLARS ON SECURITY PROGRAMS THAT WORK

Authors
Franklin S. Reeder
Daniel Chenok
Karen S. Evans
James A. Lewis
Alan Paller

October 2012

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

About CSIS—50th Anniversary Year

For 50 years, the Center for Strategic and International Studies (CSIS) has developed practical solutions to the world's greatest challenges. As we celebrate this milestone, CSIS scholars continue to provide strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a bipartisan, nonprofit organization headquartered in Washington, D.C. The Center's more than 200 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change.

Since 1962, CSIS has been dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. After 50 years, CSIS has become one of the world's preeminent international policy institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global development and economic integration.

Former U.S. senator Sam Nunn has chaired the CSIS Board of Trustees since 1999. John J. Hamre became the Center's president and chief executive officer in 2000. CSIS was founded by David M. Abshire and Admiral Arleigh Burke.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic and International Studies
1800 K Street, NW, Washington, DC 20006
Tel: (202) 887-0200
Fax: (202) 775-3199
Web: www.csis.org

UPDATING U.S. FEDERAL CYBERSECURITY POLICY AND GUIDANCE

SPENDING SCARCE TAXPAYER DOLLARS ON SECURITY PROGRAMS THAT WORK

Franklin S. Reeder, Daniel Chenok, Karen S. Evans, James A. Lewis, and Alan Paller

Overview and Summary

As the threat to the cyber infrastructure on which the federal government and the nation relies grows, the urgency of investing wisely in protection against, detecting, mitigating, and recovering from cyber events takes on increasing urgency. Our adversaries are well equipped and agile. Our defenses must be equal to the threat, and they are not.

Since the 1980s, Congress and administrations of both parties have acted periodically to address that threat, through enacting laws and issuing policies and guidance. Though the underlying principles of managing and mitigating risk remain the same, the changing nature of technology and the capabilities of those who would do us harm call for a periodic review and updating of law and policy.

Congress has recognized the need to update underlying statutes. Whether or not its efforts succeed, substantial improvement can be achieved by updating policies and guidance within the current statutory framework. Such changes would both improve our security posture and make more effective use of limited resources. While one might argue that more resources need to be spent on cybersecurity in the current threat environment, the fiscal situation argues for first assuring that every dollar spent on cybersecurity be spent wisely and allow for more rapid adoption of cheaper and more efficient technologies.

This report offers recommendations on areas where, in the view of the authors, the U.S. Office of Management and Budget (OMB) could use existing authorities and update its current guidance, last revised on November 28, 2000. These changes would make government cyber assets more secure without spending more money. Absent changes in policy, agency staff and oversight groups (e.g., inspectors general and the Government Accountability Office) will continue to waste scarce resources on strategies that do little to mitigate risk.

Our most important recommendation involves continuous monitoring of network operations. We deem this to be critical to any policy update to ensure that federal cybersecurity programs address the highest risk areas and prevent wasteful duplication of effort. Government security experts have told us that the current regime of periodic reports and certifications requires them to spend tens of millions of dollars on reports and processes that do little to enhance security. Agencies can better implement continuous monitoring through work led by chief information officers (CIOs) and chief information security officers (CISOs). This report suggests ways that OMB Circular A-130, "Management of Federal Information Resources," can be revised to enhance these activities through OMB and Department of Homeland Security (DHS) actions.

Under the current policy regime, oversight organizations, like the inspectors general and the Government Accountability Office, produce reports on compliance against outdated policies, wasting time and energy and incentivizing exactly the wrong behavior among agencies. There is hard evidence that continuous monitoring, measurement, and mitigation are far more effective in addressing real threats in an environment in which those who seek to do us harm move quickly. While agencies will still be required to report annually to OMB and Congress under the Federal Information Security Management Act of 2002 (FISMA), effective security requires that continuous monitoring, measurement, and mitigation must replace the current regime of periodic, compliance-based reporting. Changing FISMA requirements from a compliance approach that focuses on process rather than outcomes to one of continuous monitoring is the single most important action OMB can take for cybersecurity. We recommend that OMB use the authority provided under the existing statute to effect this important reform.[1]

We also recommend revisiting authority structures to reflect the reality of a changing world; namely (1) the critical role in information security for the Department of Homeland Security, which did not exist at the time OMB Circular A-130 was last revised, and (2) the need to redefine the roles and relationship between national security and non-national security systems. Although OMB further delineated responsibilities in a policy memorandum, we are encouraging OMB to address the issues in the circular's section on responsibilities.

Finally, our conversations with experts in cybersecurity revealed three other areas where, in revising Circular A-130, OMB could materially improve the effectiveness and efficiency of the federal government's cybersecurity program:

- Revising the definitions currently used and, therefore, the object of planning and review, from a technology-based (system, major application) to an information-based regime. This approach does not discount the need to analyze the components associated with the management of information, such as the network and storage locations. Agencies are ultimately accountable for protecting the information and processes for which they are stewards, whether they are on agency-operated infrastructure or in the cloud, and the policies need to reflect that. Although we do not recommend the creation of a classification scheme per se, an information-based, not technology-based, security program has allowed the national security sector to adapt much more quickly as technology has evolved.

  This is not to suggest that there is no need for rigorous physical and technology infrastructure standards in the civilian space. Rather, such continuous monitoring standards should be implemented immediately, with the goal of making them part of a broader, information-based

[1] Federal Agency Data Protection Act, Public Law107-347, Section 3543(a)(1) and Section 3543(a)(4).

framework, which is increasingly important as the government moves to virtual and cloud-based computing.

- Developing agency enterprise architectures that support the strategic, business, and technical views necessary to assist in the transition from the current state of paper compliance to a future desired state of continuous monitoring of government assets. DHS, working with OMB and the CIO Council, should have responsibility for developing a security architecture that recognizes common features across agencies, even though they have disparate missions.
- Promulgating a cybersecurity capability maturity model, much like that developed for software development. This would leverage what works best to achieve the continuous monitoring environment (and avoid deployment of a compliance model), based on real action and not the presence or absence of policies. A capability maturity model would allow the federal government as an entity to understand overall operating risk. This would provide agencies and oversight organizations a benchmark against which to measure the level to which they aspire and the steps needed to achieve it.

The changes we propose will require both modifying OMB Circular A-130 and related guidance and a change in mind-set from a compliance mentality to a true risk-based approach to deploying cybersecurity resources. Since implementing the recommendations on a maturity model and on architecture could take some time, we urge OMB not to delay issuance of an updated A-130 pending their development. Rather, we recommend that A-130 support their development.

Continuous Monitoring, Measurement, and Mitigation

> *Changing A-130 requirements from compliance to continuous monitoring is the single most important action OMB can take for cybersecurity.*

In the past few years, a new approach to cybersecurity has emerged, based on both analysis of network data and on practical experience. In this approach, continuous diagnostics and mitigation replace periodic reporting on compliance with written standards. The approach combines continuous automated diagnostic monitoring of networks for anomalous behavior with relatively straightforward mitigation strategies to address common vulnerabilities.

"Continuous monitoring" allows organizations to run programs that observe the behavior of their networks; generate quantifiable data that let them identify, report, and measure risk; and take rapid action to resolve problems. These vulnerability mitigation strategies reduce the avenues for potential attack and force attackers to develop more sophisticated (and expensive) techniques or to give up on the target. In combination, we recommend that continuous monitoring and mitigation strategies form the basis for the guidance for cybersecurity provided by A-130.

Continuous monitoring does not mean a 24-hour watch on a computer screen. This is a software-based approach that generates data and alerts by comparing network performance and configuration to specific standards and known vulnerabilities. A-130 should build on the guidance provided in the FY 2011 FISMA reporting requirements to provide a coherent system of requirements for continuous monitoring.

Continuous monitoring continues the trend of moving away from a compliance-based approach to cybersecurity to a measurement of outcomes to improve agency risk management. The compliance-based approach was expensive, insufficiently dynamic to account for threats, and did not provide managers with adequate information to make timely decisions on risk mitigation.

Automating critical controls provides daily, authoritative data on the readiness of computers to withstand attack, as well as prioritized action lists for system administrators to maintain high levels of security. At the same time, it eliminates the financial waste associated with thick audit reports that are out of date long before they are published.

In 2009, the U.S. State Department was the first agency to require wide implementation of automated security monitoring using a scoring system that gave administrators unequivocal information on the most important security actions to implement.[2] The automated security monitoring covered 85,000 computers around the world. In the first year, the risk "score" for thousands of computers across the department dropped by nearly 90 percent. In contrast, the risk scores of other federal agencies hardly changed at all. When a critical vulnerability in Internet Explorer was being exploited on Department of Defense and Department of State computers, the Defense Department took two and a half months to get 65 percent "reported" compliance with the critical patching. The State Department reached 89 percent actually patched in just 11 days.

The State Department's pioneering work in continuous monitoring has now been adapted and extended by three other government organizations: the National Aeronautics and Space Administration (NASA), the Centers for Medicare and Medicaid Services of the Department of Health and Human Services, and the U.S. Senate. At NASA, a project led by NASA Ames implemented continuous monitoring and delivered reports every few days to all the system administrators. Within days of implementation, dozens of vulnerable machines unknown to systems administrators had been eliminated from the network. Systems that were "out of mind" were never patched and thus provided a critical vulnerability; their elimination made a huge improvement in security. The entire cost of implementing the project and getting initial benefits was the time for two NASA programmers working for about eight weeks.

The Centers for Medicare and Medicaid Services (CMS) maintain information systems in nearly 200 data centers, processing claims and payments with a value of over $800 billion each year, for medical services rendered to over 100 million program beneficiaries and recipients. After

[2] In the scoring system, each automated security system—from vulnerability scanners to patch managers to antivirus managers to active directory managers and many more—feed data daily (or up to every 72 hours) into a system that converts the data into a common scoring format, an algorithm vetted by the National Security Agency (NSA). The result is a risk score for every system and for every group of systems (like those in an embassy) that can be compared and made into grades.

implementing a small pilot program, CMS used the methodology from that pilot effort to systematize the technical deployment, establish an outreach program for the remaining contractors, and implement its Continuous Monitoring and Risk Scoring (CMRS) program at additional 32 CMS sites. Many of these sites use the CMS-offered continuous monitoring tools, while others use legacy systems, connected to the CMS tool via the standardized Security Content Automation Protocol (SCAP).[3] CMS increased the total number of continuously monitored hosts from 18,000 to 46,000, while at the same time reducing average host risk scores by 83 percent.

Guidance for continuous monitoring requires identifying what to monitor, the timely collection and analysis of data, and an ability to take immediate mitigation actions. A-130 should require agencies to use standardized processes and databases for baseline security data, such as the SCAP-based data set. This guidance must be flexible enough to accommodate the "customization" of monitoring systems to different agencies' operational needs, while setting minimal controls for all agencies based on common needs.

Clearly, agencies will need to plan for a migration from the current compliance-oriented cyber regime and toward one that focuses primarily on continuous monitoring, and there will be some costs involved in this migration for which agencies need to plan. A-130 should recognize that reality; this migration could be accomplished by having agencies set timetables and resource plans against which they will be assessed, similar to how many OMB issuances address such issues. In addition, we recognize that good process is part of effective cybersecurity, and some level of reporting will continue to be necessary to demonstrate that agencies are taking basic measures to secure their networks. But given the pace of technology change, including the need to focus cyber resources on identifying and mitigating real threats and vulnerabilities that bring increased potential impacts given new technologies (e.g., cloud computing big data), we believe that focusing agency activity on continuous monitoring and not compliance is critical to achieve strong cybersecurity in the future.

Effective security requires continuous automated monitoring of agency networks for security problems, immediate access to the National Vulnerabilities Database to be able to identify problems, and immediate mitigation of problems when they are found. It does not require periodic written reports on compliance. We recommend that the centerpiece of a revised A-130 take this new approach, based on automated network diagnostics and mitigation, a comprehensive vulnerabilities database, and protocols for automated vulnerability management.

[3] Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the ways by which security information is communicated to machines and humans. SCAP is designed to organize, express, and measure security-related information in standardized ways.

Recognizing and Reinforcing the Role of the Department of Homeland Security (DHS)

DHS has spent considerable effort to build its cybersecurity program, but there continues to be skepticism about DHS's capacity. Unfortunately, this legacy continues to shape agency and public perception and is an impediment to it fully exercising its oversight functions for the federal government. More orders, statements, or guidance alone will not change this.

DHS has significantly strengthened its capacity to carry out its FISMA responsibilities. DHS will need to continue to demonstrate both capacity and accomplishment, and in our view, it is on track to do this. The assignment of FISMA authorities to DHS can only work if the department can build on its recent successes and if A-130 reinforces this by laying out explicitly the DHS role in implementing FISMA.

The administration's decision in 2010 to make DHS the focal point for FISMA implementation was a first step toward a new approach to federal information technology (IT) security. DHS's role needs to be made a central element in the implementation of a continuous monitoring, measurement, and mitigation requirement at agencies to create a fundamentally new approach to securing federal networks. A-130 should assign four tasks to DHS:

1. Recommend minimum security controls for agencies to implement, based on analysis of risks common across the government;
2. Analyze risks common across the government to recommend security controls for agencies to implement;
3. Provide this minimum control and priority list to inspectors general to help guide their assessment of agency performance; and
4. Establish a collaborative interagency process with the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) that would provide authoritative, coherent guidance for agency implementation of continuous monitoring and mitigation, based on the National Vulnerabilities Database.

FISMA responsibilities are placed in the National Cyber Security Division (NCSD) of DHS. That division has visibility into the activities of the agencies through the Federal Network Security Branch, which also oversees the Trusted Internet Connection (TIC) implementation in each agency. However NCSD's mandate also includes incident response for all agencies and other services, which takes a great deal of time and attention from management. While the internal structure of DHS is beyond the scope of A-130 and this report, we believe that if DHS were to separate its tactical, operational functions from its management oversight responsibilities (e.g., FISMA), this separation would allow a greater focus on rapid reduction of vulnerabilities across the government.

Revisiting the National Security-Civilian Dichotomy

As the CSIS Commission on Cybersecurity for the 44th Presidency noted in its 2008 report, "the historic distinction between civilian agency systems and national security systems no longer serves the U.S. interest."[4] Originating in the Computer Security Act of 1987, this split has served to ensure that efficiency and privacy interests in the civilian space are not overtaken by more stringent standards commonly associated with national security systems.

In today's cyber environment, both threats and vulnerabilities travel across the federal space in real time, calling for close coordination in response. Such coordination ensures that there are not different levels of effectiveness in protecting federal systems based solely on which agency responds to a common cyber incident. At the same time, the authors support the important privacy and civil liberties interests that any agency, whether civilian or national security, should respect in addressing security.

The historic distinction between national security systems and non-national security systems, however, is an anachronism. The distinction between civilian agency systems and national security systems creates a gap that attackers can exploit to enter and damage government systems or gain access to highly sensitive information. Our adversaries understand this. Our policies and structures need to reflect this reality.

The Obama administration has taken a number of steps to operationalize greater coordination of cybersecurity policy across the civilian and national security spaces. Two examples are the cross-placement of DHS and NSA staff under the October 2010 Memorandum of Agreement, and the creation of a committee to coordinate standards development across NIST and NSA.[5]

We recommend that OMB policy should base cyber policy and response on level of risk rather than agency source—similar to the principles that were laid out in OMB M-04-04 on authentication, which also required that privacy be addressed at each risk level. This policy established four hierarchical "levels of assurance," with each level requiring more stringent actions. OMB should use A-130 to initiate a similar government-wide policy based on assessments of vulnerability and threats to mission outcomes. Where the agency mission involves sensitive information, this policy could instruct agencies to implement stronger security with more extensive protections. Other, less sensitive missions would emphasize open access and transparency.

[4] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency* (Washington, DC: CSIS, December 2008), p. 70, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

[5] The Joint Task Force Transformation Initiative, a partnership with NIST, the Department of Defense, the intelligence community, the Office of the Director National Intelligence, and the Committee on National Security Systems, is tasked with developing a unified information security framework for the federal government.

Because the current statutory framework calls for a two-track security policy, we recommend that A-130 set forth in policy the goals that similar risks should be handled with similar approaches, regardless of the category into which the agency at risk falls. Specifically, A-130 should indicate that the process started under the Joint Task Force Transformation Initiative should continue.

Finally, we recommend that A-130 require each agency that addresses cybersecurity at given levels of risk to ensure that privacy and civil liberties are addressed from the onset, as well as at each stage of agency implementation of its cyber program. Privacy could be protected at all levels through requirements for Privacy Impact Assessments and the application of Fair Information Principles under the Privacy Act.

Definitions

OMB Circular A-130, titled "Management of Federal Information Resources," is aptly named as information is the federal government's largest asset. Appendix III addresses security for federal automated information resources. There is one definition that through the years of use has caused confusion on what should be included and what should not be included in oversight. Currently, the definition of "major information system" is an information system that "requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property or other resources." This definition as currently written was meant to give agencies flexibility in determining how to develop their portfolio and investments for information technology.

However, as agencies take advantage of the efficiencies of technology, costs should be much lower because agencies can combine information resources to deliver a service, without creating new hardware or software assets—which also means that the "system" may not rise to the level of oversight or considered to be "included" in the overall management of departmental assets. We recommend a new definition to continue to allow flexibility for agencies, but also allow for a common understanding by all parties of what goes into a system. This revised definition should be consistent with the Clinger-Cohen Act and FISMA definitions of "information system," which is "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."[6]

The proposed definition would include and/or build from the FIPS-199, Standards for Security Categorization of Federal Information and Information Systems.[7] By looking at the categories of

[6] Information Technology Management Reform Act, 44 USC 3502(8).

[7] National Institute of Standards and Technology, "Standards for Security Categorization of Federal Information and Information Systems," Federal Information Processing Standards (FIPS) Publication 199, February 2004.

information to include confidentiality, integrity, and availability, the definition of major information system could be modified along the following lines:

> A "major information system" is one in which compromise of any of the security objectives—confidentiality, integrity, and availability (44 USC, SEC 3542)—have been rated to have a severe or catastrophic adverse effect on organizational operations (FIPS 199, Table 1) or where compromise could put significant financial resources or investments at risk.

In addition, A-130 could clarify that the definition of "information system" under Clinger-Cohen does not mean a static set of resources, but rather can change over time and thus requires continuous management attention—which reinforces the importance of continuous monitoring of the various sources that flow in and out of the "information system."

Taken together, these two changes would focus the attention to the "information" itself, as opposed to the technology and application being used to supply or create the information. The shift of the focus to information recognizes the constantly changing technology environment and allows agencies to take advantage of the most up-to-date solutions, while taking into consideration the risk associated with their deployment. Additionally, this only assists in prioritizing the overall review of information resources. The approach would need to be used in conjunction with the "continuous monitoring" in order to adequately assess the risk profile associated with the agencies' services.

Security Architectures

The development of agency security architectures is essential to achieve this shift from "systems" to a total focus on "information." Most agencies should have their current state mapped out ("as is"). The shift to "information" eliminates the barriers and borders of information technology systems and would have the agencies map the use of the information in their target architectures ("to be"). This shift is critical in order to have "continuous monitoring" really work. The architectural efforts will assist the agencies in transition from managing configurations today to managing risk levels of information into the future with the shift to cloud services. Initiatives such as the Federal Risk and Authorization Management Program (FedRAMP) will then allow for agencies to rely on the security being established at an agreed upon risk level with associated security settings that align with the architecture. The use of this approach to testing of security settings should also be expanded beyond just "cloud services," in order to allow agencies to focus on their mission specific needs. Continuous testing/monitoring will then be able strengthen agency risk postures, facilitated by testing for a range of IT applications prior to being approved for use.

Security Capability Maturity Model

In order to truly strengthen the nation's security posture, it is imperative that we shift from the compliance methodologies to true performance outcomes. To reduce risk, the entire department and/or agency needs to be involved. The development and implementation of a security capability maturity model, and rigorous scoring against that model, would recognize the differences among agencies and reinforce the need for continuous improvement. This model would provide a more meaningful basis for the inspectors general independent annual evaluation of FISMA and assist in shifting from the current paperwork to real outcomes. By taking the current NIST standards, FIPS publications, and other available policy documents, one could design a capability maturity model around:

- Assets: measure/test actual settings; inventory, etc.;
- Events: ability to respond to cyber events;
- People: what are roles and responsibilities?

A capability maturity model would measure progress toward achieving the risk levels established as "acceptable." Progress can also be measured along technical and process dimensions. The key to success will be to avoid the mistakes of past models and measurements of cyber security, to ensure we are raising the bar and not just providing another method of compliance, in order to achieve a truly improved cybersecurity posture as a nation.

Conclusion

The current policy and legislative framework for protecting our nation's cyber infrastructure needs updating and revision. It is our view that the administration, and OMB in particular, have ample legal authority to adopt reforms that would materially reduce risk and enhance response for systems operated by or on behalf of the federal government.

About the Authors

Franklin S. Reeder, a former official with the Office of Management and Budget, is cofounder and director of the Center for Internet Security and the National Board of Information Security Examiners. He served on the CSIS Commission on Cybersecurity and, with Karen Evans, coauthored the Commission's white paper on the cybersecurity workforce, *A Human Capital Crisis in Cybersecurity* (CSIS, November 2010).

Daniel Chenok is executive director of the IBM Center for the Business of Government and chair of the Information Security and Privacy Advisory Board. He was a member of the CSIS Commission on Cybersecurity and worked in the Office of Management and Budget, where he led the Information Policy and Technology Branch that oversaw policy and budget for technology, computer security, information policy, and related issues.

Karen S. Evans serves as national director for the U.S. Cyber Challenge, a nationwide program focused specifically on the cyber workforce. She serves as a voice of authority for Safegov.org, an online forum focused on cloud computing policy issues. She retired after nearly 28 years with the federal government, including service as administrator for e-government and information technology at the Office of Management and Budget, where she oversaw the federal information technology budget of nearly $71 billion.

James A. Lewis is a senior fellow and director of the CSIS Technology and Public Policy Program. His recent work has focused on cybersecurity, including the groundbreaking report *Securing Cyberspace for the 44th Presidency* (CSIS, December 2008). His current research examines the political effect of the Internet, strategic competition among nations, and technological innovation.

Alan Paller founded and is director of research at the SANS Institute, a college and professional cybersecurity training school. He oversees the Internet Storm Center, the annual identification of the "Seven Most Dangerous New Attack Vectors." He also cochairs the Department of Homeland Security Task Force on Cyber Skills and serves on the Federal Communications Commission's Communications Security, Reliability and Interoperability Council.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1800 K Street, NW | Washington, DC 20006
Tel: (202) 887-0200 | Fax: (202) 775-3199
E-mail: books@csis.org | Web: www.csis.org