Measuring What Matters:

Reducing Risk by Rethinking How We Evaluate Cybersecurity

March 2013

Julie M. Anderson
Karen S. Evans
Franklin S. Reeder
Meghan M. Wareham

SafeGov

Report Authors

Julie M. Anderson, *Chief Operating Officer of Civitas Group*
Karen S. Evans, *National Director of the U.S. Cyber Challenge**
Franklin S. Reeder, *Director of the Center for Internet Security **
Meghan M. Wareham, *Senior Associate at Civitas Group*

Academy Panel

Earl E. Devaney, *Chair**
Douglas T. Robinson*
Ramon C. Barquin, Ph.D.*

Academy Project Team

Joseph P. Mitchell, III, Ph.D., *Director of Project Development*
Jonathan C. Tucker, Ph.D., *Project Director*
Daniel Caravalho, *Research Associate*

This is a report of the authors, not the Academy Panel or the Academy as an institution.

March 2013

*Academy Fellow

Message from a Panel of the National Academy of Public Administration

Increasingly sophisticated cyber attacks threaten the security of federal information systems, but the federal government's current approach to security and privacy assessments of its information systems hinders an effective response to this dynamic threat. Current policies encourage compliance-oriented assessments as opposed to enterprise-oriented risk mitigation, continuous monitoring, and measurement.

SafeGov has developed a framework to spur the creation of a more effective approach to cybersecurity evaluation. As part of its strategy for developing this framework, SafeGov engaged the National Academy of Public Administration ("the Academy") to convene an expert Panel of its Fellows to conduct an independent review of the framework.

Based on its review, the Academy Panel believes that the cybersecurity evaluation framework developed by SafeGov in this report is an important step toward building a more dynamic, risk-based approach that will yield more robust protection from cyber threats across the government. A key strength of this approach lies in the tools it suggests to IGs and agency management to ground their assessments and decision-making on common standards and methodologies. If implemented, this tools-based approach will help enable consistently higher levels of protection across the government, while enabling flexibility in its application to the diverse circumstances of federal departments, agencies and programs.

While the Panel supports the intent of this effort, it believes that successful implementation depends on:

- Additional stakeholder outreach to refine and build support for the framework;
- Planning to address significant administrative challenges.

Additional Stakeholder Outreach

Further outreach should include three stakeholder groups: (1) Inspectors General; (2) Congress; (3) and state government officials. First, SafeGov engaged only a very small sample of IGs during the development of its framework. Given the diversity and critical importance of IGs to the initiative's success, it is essential to engage this group more fully.

Second, although the SafeGov framework was deliberately designed to be implemented without the need for new legislation, it is still important to engage congressional stakeholders to address any concerns that the framework is not in keeping with congressional intent. Also, as the framework is further developed and implemented it may become clear that some changes in statute or regulation would be helpful. Engaging congressional stakeholders at this early stage will help ensure buy-in and support for needed changes down the road, as well as support for addressing challenges to successful implementation, such as access to the right skill sets and additional resources or reprioritization of existing resources.

Third, state governments and CIOs, in particular, are an important stakeholder group to engage given their role as implementers of federal programs, many of which are covered by FISMA. States deliver over $550 billion in diverse federal programs to citizens—ranging from Medicaid, support for families, homeland security, unemployment and education. A portion of these funds are used for information systems that states purchase, develop, implement and make secure to carry out the federal programs. The states will be affected by changes in the approach to cybersecurity assessments flowing from the adoption of SafeGov's framework. They can help identify implementation challenges and their active support will be important for success.

Administrative Challenges to Address

Administrative challenges to be considered in implementation planning include: (1) the culture of IGs and agencies; (2) gaps in the skill sets of IGs and agencies; (3) reallocation of existing resources and, potentially, obtaining additional resources; and (4) contracting arrangements. Moreover, clear and explicit guidance from OMB will be a critical factor in addressing these challenges.

First, moving from compliance-based assessments to enterprise-oriented risk mitigation, continuous monitoring, and measurement will entail a major cultural shift on the part of IGs as well as agencies. While the tools that would be provided under the SafeGov approach will facilitate the shift, ultimate success will depend on strong leadership and careful attention to incentives.

Second, IG and agency personnel do not always have the skills required by the new approach. Steps must be taken to ensure that IGs and agencies can marshal the right mix of skills whether through hiring and training internal personnel or contracting for the appropriate expertise.

Third, given the near-term budget environment, it is unlikely that new resources will be available to implement the shift to the new approach, which means that existing resources must be reallocated. Cybersecurity has not been a top priority of IGs generally. Leadership from OMB will be required to ensure that cybersecurity becomes a priority of IG leadership and that resources are reallocated accordingly.

Fourth, timely, effective, and secure contracting arrangements will be very important in helping ensure that IGs and agencies are able to access the skill sets needed to implement the framework. Careful consideration should be given to making sure that existing contracting arrangements will meet the needs of effective implementation. FedRAMP offers at least a partial precedent that should be examined more fully in this regard.

In conclusion, the Panel believes that this framework will help set federal cybersecurity improvement efforts on the right path and promises greatly improved risk management as well as more efficient use of increasingly constrained government resources. However, further stakeholder outreach and careful implementation planning are required for success.

Academy Panel of Fellows

Earl E. Devaney, Chair
Former Chairman, Recovery Accountability and Transparency Board and Inspector General, Department of the Interior. Prior positions include: Director, Office of Criminal Enforcement, Forensics and Training, Environmental Protection Agency; Special Agent in Charge, United States Secret Service.

Ramon C. Barquin, Ph.D.
President, Barquin International. Prior positions include: President, Washington Consulting Group; Manager, Public Affairs Programs, IBM; Manager, External Programs, World Trade Asia, IBM; Manager, External Programs & Marketing Research, Americas/Far East Corp., IBM. Former President, The Data Warehousing Institute. On the Board of the Center for Internet Security.

Douglas T. Robinson
Executive Director, National Association of State Chief Information Officers. Prior positions include: Executive Director, Policy & Customer Relations, Technology Office, Governor of Kentucky; Consultant, Information Technology Management; Former positions with Finance & Administration Cabinet: Executive Director, Kentucky

Information Resources Management Commission; Executive Director, Kentucky Office of Geographic Information Systems.

Table of Contents

"What gets measured gets done."
Tom Peters April 28, 1986[1]

"Not everything that counts can be counted, and not everything that can be counted counts."
from a sign that reportedly hung on Albert Einstein's office wall

Executive Summary

In the past ten years, Federal agencies have worked to improve the security of information and information systems. Despite the guidance of experts and millions of taxpayer dollars, Federal information systems remain critically vulnerable to breaches and cyber-attacks. As government agencies fail to implement needed improvements to information security management, they continue to spend scarce resources on measures that do little to address the most significant cyber threats.

This report offers a different approach to reducing risk: the Organization Cyber Risk Management Framework. The proposed framework draws from the ongoing work of several federal agencies, including the National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Office of Management and Budget (OMB), Department of Energy (DOE), and the General Services Administration (GSA), and proposes the creation of an Organizational Cyber Risk Indicator. The Organizational Cyber Risk Indicator assesses the cyber risk posture of a government organization by aggregating the results of Inspectors General (IG) Federal Information Security Management Act (FISMA) evaluations into an established formula. By using this indicator, along with a more dynamic evaluation process, agencies will be better able to counteract existing vulnerabilities and improve overall risk management.

This approach will strengthen the security of government information systems and improve the overall management of government resources by focusing scarce resources on the areas that pose the highest risks to agencies' missions.

[1] Also attributed to Peter Drucker, among others.

Before implementing this approach, however, agencies must demonstrate the ability to operate and manage a cybersecurity and data protection baseline. This secure baseline includes:

- Critical security controls; and,
- Automated continuous monitoring, diagnostics and mitigation.

Cybersecurity can be thought of as analogous to basic health standards. Just as we understand the value of washing one's hands, there are certain "hygiene" practices in cybersecurity that are critical to protecting against known vulnerabilities. In order to avoid radical and expensive measures (such as quarantining a vulnerable computer network), firms and agencies can protect themselves by adopting these baseline practices.

Recommendations

To better secure information and improve information security evaluations across government, the report team recommends OMB direct the following policy changes:

1. IGs should adopt the enhanced risk management framework and submit a FISMA Evaluation Plan to OMB by no later than May 2013;

2. NIST should include the enhanced risk management framework, including the cyber risk indicator concept, to foster a more evidence-based and outcome-oriented approach to evaluating information risk management;

3. NIST, in coordination with DHS, should develop and incorporate a clear threat model as a part of the cybersecurity framework to build a foundation for risk management across agencies. This will allow agency leaders to better and more consistently discern what risks can or cannot be accepted;

4. IGs should prioritize their findings in accordance with the agency or department's defined risk level and also distinguish between managerial and technical controls;

5. Agency Chief Information Officers (CIOs) should lead the effort to integrate the IG's findings into overall department or agency strategic mission priorities, processes, and decisions; and,

6. GSA should expand the Federal Risk and Authorization Management Program (FedRAMP) program beyond cloud services.

The development of this framework has been guided by the following principles:

1. Promote performance outcomes in the place of compliance methodologies through the creation of metrics that map to the performance of information security and data protection controls.

2. Strengthen the development of robust risk management and incident response mechanisms by defining agency risk from an enterprise perspective.

3. Institutionalize behavior such as continuous monitoring that address gaps in systems as they appear.

4. Create a cybersecurity and data protection assessment system that encourages innovation and remains flexible to deal with technological change.

5. Coordinate with previous and ongoing work of NIST, DHS, DOE, SANS Institute, the Center for Strategic and International Studies (CSIS), and international bodies such as the International Standards Organization (ISO).

Conclusion

FISMA was designed to address and mitigate the cybersecurity threats facing Federal departments and agencies. However, because of shortcomings in the way FISMA has been implemented, existing policy has not always promoted the achievement of desired results. Current FISMA evaluation policies and processes do not, in sum, enhance our government's cybersecurity posture. To fix the problems of today without losing sight of the future, government should implement a more consistent method of evaluation--one which is measurable, transparent, and outcome-oriented. As long as policy guidance falls short and evaluation methods fail to assess what security and data protection mechanisms significantly reduce risk, government will continue to spend scarce taxpayer resources doing the wrong things.

Introduction

As technology advances and potential adversaries become more capable, cyber-attacks pose a growing threat to the security of government information. Unfortunately, current government policies and processes are not measuring activities that address this dynamic threat. Work is being done, but is it the right work?

Under FISMA, each Federal agency is required to develop, document, and implement an agency-wide program to secure its information systems, including those supported by outside contractors. As part of this program, agencies must identify an acceptable level of risk for their information systems and develop the attendant policies, procedures, and security plans to reduce information security risks to an acceptable level in a cost-effective way. Under FISMA, IGs of the various Federal departments and agencies are required to perform annual, independent assessments to determine the efficacy of these practices.

OMB provides annual guidance to assist the IGs in performing FISMA evaluations. Unfortunately, the implementation of existing security and privacy assessment policies tends to encourage security officials to spend limited cybersecurity resources on measures that do little to enhance the security of information systems. The Federal government's approach to evaluating FISMA compliance relies on process-oriented methods that focus on the completion of checklists rather than on whether agency cybersecurity programs measurably improve the security of Federal IT assets. The current evaluation system fails to reward agency leaders who make well-measured, risk-based decisions to guide IT investments and improve the security of government information. This stems from the fact that current OMB guidance fails to distinguish between the trivial and important.

This new evaluation approach—the Organizational Cyber Risk Indicator—provides a quantitative measure for assessing cyber risk in Federal government agencies by aggregating the results of IG FISMA evaluations into an established formula. The use of this indicator—combined with a more dynamic evaluation process—will promote a more consistent methodology for assessing cyber risk across Federal agencies. In turn, it will encourage agencies to define their risk profile in a strategic, enterprise-wide manner that supports their programmatic missions and goals. This approach will strengthen the security of government information systems and improve how government resources are managed by focusing resources and attention on the areas that pose the highest risks to agencies' missions.

This report provides an overview of the framework; identifies key principles, recommendations, and challenges to implementation; and considers the potential value of this revised approach. It is intentionally written to spur debate in hopes of influencing policy guidance for FISMA evaluations in the coming years. The implementation of this framework is not contingent on legislation. It is also consistent with the current effort underway at NIST to create a cybersecurity framework for critical infrastructures in the United States, mandated under Executive Order 13636.[2] The approach proposed in this report should be reconciled with the NIST framework once it is established.

Organization Cyber Risk Management Framework Overview

The framework is designed to foster continuous feedback among agency leaders, IGs, and other oversight organizations. It does this by linking the central features of any comprehensive cybersecurity strategy (including agency threat assessments, risk mitigation action plans, information security management, and recommendations from IG information security evaluations) to agency cybersecurity investments and strategic management.

Moreover, to ensure that concerns are identified during the research and stakeholder outreach processes, the report team identified a number of necessary steps that must be completed prior to moving to the risk management framework approach recommended in this report. These steps include, at a minimum, the capabilities such as automated continuous monitoring that departments and agencies need to implement to create a secure baseline for information and information systems security.

In order to establish a secure baseline, agencies and departments must first implement automated continuous monitoring programs. These include continuous diagnostics and

[2] Executive Office of the President, *Executive Order on Improving Critical Infrastructure Cybersecurity*, February 12, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

mitigation, configuration management, threat assessment, and remediation practices in accordance with established DHS procedures. In addition, the secure baseline should also include Critical Security Controls aligned with the NIST Special Publication (SP) 800-53 v4, "Security and Privacy Controls for Federal Information Systems and Organizations." This secure baseline could be updated as automated information security capabilities advance.

Agencies and departments can use this enhanced risk management framework regardless of statutory and regulatory changes, as the framework incorporates fulfillment of agency and department regulatory obligations as one of the dimensions for evaluation.

Before implementing this approach, agencies must establish and demonstrate that they can manage a cybersecurity and data protection baseline by implementing:

- Critical security controls; and,
- Automated continuous monitoring, diagnostics and mitigation.

Cybersecurity can be thought of as analogous to basic health standards. Just as we understand the value of washing one's hands, there are certain "hygiene" practices in cybersecurity that are critical to protecting against known vulnerabilities. In order to avoid radical and expensive measures (such as quarantining a vulnerable computer network) firms and agencies can protect themselves by **adopting these baseline practices.**

As highlighted in the annual FISMA report released in March 2013, the areas in greatest need of improvement include continuous diagnostics and mitigation, configuration management, threat assessment, and remediation practices.[3] Departments and agencies must better counter current threats that exploit common vulnerabilities against federal government assets and their respective support contractors. Doing this requires implementing technical controls that align with the NIST DRAFT SP 800-53, v4, such as the Critical Security Controls.

[3] Executive Office of the President, *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. March 2013, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

Once these baseline practices are in place, agencies should develop a clear understanding of the threats they face in their current operating environment, and how those threats could be realized. A strong threat model, which includes an agency's current and future operating environment, is critical to any effective risk management strategy. Once the threat model is developed and applied, agency leaders should identify key organizational mission priorities and map these priorities to critical assets. Only by defining organizational mission priorities, known threats, and critical assets can agencies determine their desired risk profile and the appropriate controls required to address those threats.

Different agencies will face different threats and must, therefore, tailor their risk mitigation strategies to their individual needs. The public health analogy works here as well. Some of us need to do little more than engage in good personal hygiene (the baseline), while a few of us who are more at risk need to take additional steps to protect ourselves and the larger community.

In the second phase, IGs will be able evaluate the maturity of the processes associated with information security, threat mitigation, and risk management based on the department or agency's chosen risk attributes and security controls. This evaluation is not intended to preclude an IG from evaluating the efficacy of the agency's risk profile decisions. The evaluation process will be outcome-oriented, draw upon live and scenario-based tests of information systems, and result in a prioritized list of recommendations for risk mitigation. It is intended to facilitate communication within agency management, especially among CIOs and the IGs, to address the identified deficiencies. The evaluation will be conducted across ten separate domains of information management to acknowledge the interconnections between technical capabilities, organizational policies and processes, and personnel capabilities. The ten domains include asset, change, and configuration management; access management; identity management; data management and protection; threat and vulnerability management; situational awareness; information sharing; workforce and external dependencies management; incident response, monitoring, and Continuity of Operations (COOP) Planning; and program management. These domains will be explored in greater detail later in this document.

In the final phase, security officials will calculate an organizational cyber risk indicator by using a formula that aggregates the measured outputs of the IG evaluation process.

The cyber risk indicator reflects the capacity of an agency to manage threats based on their existing operating environments and organizational priorities. Agency leaders can then use this cyber risk indicator alongside a list of prioritized risk mitigation recommendations to address ongoing vulnerabilities and improve how they manage risk and implement information security controls. By making agency leaders more aware of the evolving threat environment and their own risk mitigation capabilities, these processes will help them make better operational decisions, more effectively target their information security investments, and plan for the future more strategically.

Recommendations

By implementing the following recommendations, Federal departments and agencies can reduce and better manage their operating risk on a continuous basis. In order to ensure implementation, OMB should direct the following activities through policy guidance:

1. IGs should adopt the risk management framework evaluation approach requiring them to submit a FISMA Evaluation Plan by no later than May 2013. The plan should include, at a minimum, the methodology by which the IG would evaluate the following:
    a. Verification of the agency's baseline capabilities;
    b. Implementation for diagnostic continuous monitoring as described by DHS; and,
    c. Implementation of prioritized critical security controls.

2. NIST should include in its guidance the principles and approach of the enhanced risk management framework, including the cyber risk indicator, to foster a more evidence-based and outcome-oriented approach to evaluating information risk management;

3. NIST, in coordination with DHS, should develop a clear threat model as a part of the cybersecurity framework to build a foundation for risk management across agencies, which will allow agency leaders to better and more consistently discern what risks can or cannot be accepted;

4. IGs should prioritize their findings in accordance with the agency or department's defined risk level and also distinguish between managerial and technical controls. IGs should also use a more continuous evaluation approach;

5. Agency CIOs should lead the effort to integrate the IG's findings into overall department or agency strategic missions. CIOs should address prioritized IG findings to achieve the risk level commensurate with the nature of their information assets in a clear and transparent way; and,

6. GSA should accelerate the adoption of the FedRAMP program beyond the cloud services to other operating environment and services. FedRAMP's governance process program, combined with the use of independent Third-Party Assessment Organizations (3PAOs), provides a consistent, transparent methodology with established technical security controls that both the government and potential contractors understand. The 3PAOs or an equivalent type of entity should conduct the actual testing of departments and agencies' operational security controls and provide their results to the IGs for inclusion in their evaluations.

Methodology for this Study

In developing this framework, the project team used an iterative and collaborative approach to leverage the input of more than twenty senior government and industry IT leaders. The team began by creating a draft framework that identified key themes for discussion by drawing from the work of multiple entities, including NIST, DHS, DOE, GSA, and OMB. These agencies and other organizations are already working to improve cybersecurity and data protection measurement and evaluation practices (see Appendix A: Current Environment, for an illustrative list of efforts that should be leveraged in the further development of this framework). The draft framework was shared with key stakeholders, including government policy makers and technical experts, private industry experts, association representatives, and subject matter experts working in non-governmental organizations.

Within the scope of the effort, the team included the potential implementation effects on the federal government and their information technology (IT) support contractors.

Finally, recommendations from a panel of experts from the National Academy of Public Administration ("the Academy") who reviewed the framework were incorporated into this final report.

The development of this framework has been guided by the following principles:

1. Promote performance outcomes in the place of compliance methodologies through creation of metrics that map to the performance of information security and data protection controls.

2. Strengthen the development of robust risk management and incident response mechanisms by defining agency risk from an enterprise perspective.

3. Promote institutionalization of behaviors such as continuous monitoring that address gaps in systems as they appear.

4. Create a cybersecurity and data protection assessment system that encourages innovation and remains flexible enough to deal with technological change.

5. Align efforts with previous and ongoing work of NIST, DHS, DOE, SANS Institute, CSIS, and international bodies such as ISO.

Desired Outcomes

The purpose of the approach proposed in this paper is to reduce cyber security threats that exploit common vulnerabilities of agencies' information systems, thereby helping them discharge their responsibilities to the American people, whether that is defending the nation's security or issuing Social Security payments.

The risk management framework concept promotes greater dialogue and cooperation between government and industry entities to create a more effective method for evaluating how FISMA and other associated statutes and policies are implemented. An improved evaluation process will help the U.S. Government better secure its information and information systems and manage resources. By establishing a secure baseline,

adopting the enhanced risk framework for continuous risk assessment, and calculating an organizational cyber risk indicator for each department and agency, Departments and agencies will create:

1. An approach to evaluating agencies' risk management capabilities that is evidence-based and outcome-oriented.

2. An evaluation framework that ties most closely to organizational priorities by defining necessary actions.

3. An enterprise-wide strategic risk profile, to be used by senior management to support their policy and programmatic decisions, thereby strengthening the security of government information systems and improving the overall management of government.

4. A flexible cybersecurity and data protection assessment system that can adapt to future technological and regulatory change.

5. A more consistent and prioritized process of evaluation that can feed to other aspects of agency planning and increase efficiency, ease, and utility of IG assessment processes.

Overview of Existing Evaluation Process

The existing FISMA evaluation process has been undermined by a lack of alignment between agencies and IGs. Despite the intentions of FISMA, agencies do not universally evaluate risk and threats in an enterprise-wide manner. This leaves IGs to complete the evaluation using the NIST Special Publications but without agency-specific guidance or a standardized methodology that considers how agencies address risk at a department-level. Moreover, IGs apply significantly different criteria in assessing and evaluating the security of information systems. While some IGs perform live tests and write targeted evaluations, others emphasize policy and governance issues over determined results. In other cases, IG reports lack clear priorities for agency action, stressing compliance over risk management. For example, one Federal agency noted that in a recent FISMA evaluation, **IG findings ranged from the need to cover a power outlet to deficiencies in**

configuration management. Unless these recommendations are prioritized, agencies are left without a clear sense of where to start and where to invest valuable resources.

To be sure, some IGs are exceptions to this rule and demonstrate best practices in risk management. These best practices should be more systematically leveraged in implementing this new approach.

Federal IT stakeholders also have critiqued the relative subjectivity of yearly FISMA guidance, as well as the dearth of specific criteria for assessment. Each year, IGs receive specific guidance from OMB designating areas of focus for the FISMA evaluation. While these annual changes in evaluation criteria reflect important advances in terms of Federal information security initiatives, they should be enhanced and more frequently updated to provide for a continuous cycle of organizational assessment and improvement.

During the congressional hearing held on March 7, 2013, the Government Accountability Office (GAO) found improper usage, malicious code, and unauthorized access were the most widely reported types of attacks across the government. Greg Wilshusen, Director of Information Security Issues for GAO, commented: "*This is why we've been designating information security as a high risk area since 1997…because agencies, I wouldn't say [due to] their inability,* ***but [because of] their lack of meaningful success*** *in securing their systems and meeting many of the requirements for securing their systems" [emphasis added].*

As an example of existing best practices, a recent IG report from the Department of Veterans Affairs (VA) acknowledged that agency management had evaluated the risks of transmitting certain data over unencrypted lines. The IG criticized this decision, asserting that it was made with little regard for potential vulnerabilities associated with the sensitivity of the information at hand.[i]

i. VA Office of Inspectors General, "Review of Alleged Transmission of Sensitive VA Data Over Internet Connections," March 6, 2013, http://www.va.gov/oig/pubs/VAOIG-12-02802-111.pdf.

An Organization Cyber Risk Management Framework

Overview

The risk management framework concept proposes significant changes to the ways in which agencies build their cybersecurity programs and IGs conduct information security assessments under FISMA. The changes are designed to encourage agency leaders to evaluate their risk profiles based on enterprise information holdings rather than merely according to information systems. In doing so, it delineates a clear set of tools for IGs to leverage in providing coherent, actionable and outcome-oriented recommendations to agency IT leaders.

The risk management framework is designed to build upon existing FISMA and NIST guidance and encourage a dynamic cycle of risk management and mitigation between agency leaders and IGs. In the framework, significant responsibility lies with the agencies' management teams and ultimately the agency heads. By identifying their organization's priorities and desired risk levels for key information systems, they provide IGs with the foundation necessary to evaluate information security management. Moreover, agencies are also responsible for reviewing IG findings and using their recommendations to improve how information is managed and secured.

Technical Framework

The risk management framework closely integrates the efforts of agency leaders and IGs to help create a reiterative, dynamic process that integrates information security management into the broader strategic management and budgeting process.

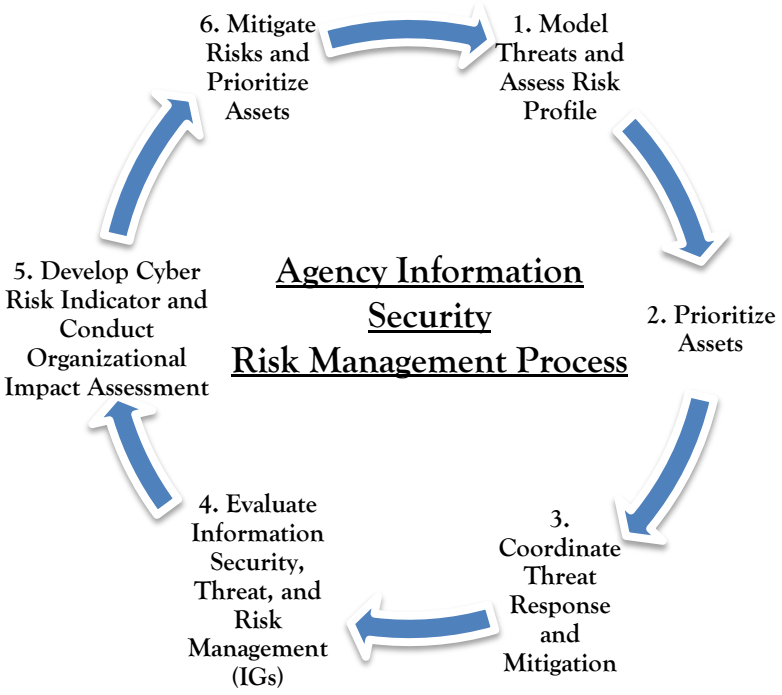

Figure 1. "Agency Information Security Risk Management Process."

The framework draws upon existing processes and new methods of evaluation to produce clear, prioritized results.

Agency Risk Profile Assessment and Asset Prioritization

Under FISMA, agencies are directed to implement information security controls based on the risk level of their information systems. In an updated risk management process, agency leaders would re-emphasize the organization-wide security program required to tie the process of planning and implementing information security to the organization's wider strategic and investment efforts.[4] On an annual basis, agency leaders should also report on their organizational priorities, including but not limited to critical services and processes, physical assets, and stakeholders tied to fulfilling their mission. These organization priorities should be mapped to specific, prioritized information assets. This mapping should dictate the designated risk profile for the core assets of each

[4]See NIST Special Publication 800-37, Revision 1, describing the six steps of Risk Management Framework. [U.S. Department of Commerce. *NIST Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf].

agency, which may differ across information systems depending on how critical they are to mission fulfillment, as well as other regulatory or national security standards. Using this risk profile assessment, agencies should identify and implement appropriate information security policies, processes, and controls.

In order to establish a department or agency's baseline capabilities, leadership must also consider the follow key elements:

1. ***Shift from a "system" approach to an "information" approach*:** Currently, cybersecurity is thought of in terms of "information technology systems," which sets technologists apart from the mission owners. By shifting to an information-centric view, agency leaders will be better able to address the risks associated with the information itself. For example, agencies currently develop plans of action and milestones (POAMs) for each individual "system" within their organization. In theory, the IG should be able to map all POAMs to an overall enterprise risk profile as determined by the management team as depicted in Figure 2, "The Organization Cyber Risk Management Framework." While the organization may have established a "perimeter defense," a coverage gap surfaces whenever information flows from one "system" to another, such as when human resources information is sent from a payroll system to a financial management system. What happens and who is responsible when the information travels between the two systems? By shifting from a "systems" approach to a more integrated and holistic "information" perspective, agency leaders can better emphasize "data protection" and address multiple policies and statutes including the Privacy Act and FISMA, among others.

2. ***Multi-dimensional, consistent performance measures*:** In order to leverage models from the past, any new approach should combine attributes that allow for measurement and flexibility within and among departments and agencies. For example, the existing FedRAMP program can be expanded to include the baseline capabilities of agencies in deploying services. The FedRAMP program determined the technical controls for both low and moderate security levels for cloud providers. It also developed the standard templates and described the data needed to demonstrate the capability. The evaluations are completed by independent contractors (3PAOs) in a consistent, repeatable way. Additionally, the 3PAOs continuously test after the agency has deployed within the cloud

provider to ensure the same controls are maintained. The leading practices adopted in FedRAMP, including the joint governance board in place, could be expanded to assess the cyber risk of the organization using the same approach. IGs could employ the FedRAMP model to conduct financial audits each year, using the 3PAOS or equivalent organizations to test operational security controls. For example, consider an agency that has deployed a financial management IT system. When the organization is audited, the IT component of the audit gets tested according "Generally Accepted Accounting Principles (GAAP)." In this context, the audit could include new standard templates and measures for consideration into the Federal Accounting Standards Advisory Board (FASAB) process, which will be measured consistently throughout the enterprise regardless of whether it is a financial audit or a FISMA evaluation.[5]

3. ***Creation and use of standard templates*:** Data that is gathered consistently according to standard templates is more valuable by virtue of being clearer, more reliable and more easily compared to other data. When the framework concept is adopted, it will illustrate the overall community risk imposed or reduced by a particular agency or department. By providing consistent, standardized methods for oversight, the framework resolves conflicts between CIOs and IGs over how to evaluate organizational risk.[6]

IG Information Security Risk Management Evaluation

By incorporating an agency's risk profile assessment and information security asset prioritization, IGs can evaluate their agency's security risk in a more targeted, results-oriented manner. This process would assess how well an agency is managing risk across ten information security and data protection domains:

1. Asset, change, and configuration management;
2. Access management;
3. Identity management;
4. Data management and protection;

[5] See Appendix A, "Current Environment," for an in-depth discussion of the potential use of government financial audit practices in information security evaluations.
[6] See Appendix A, "Current Environment," for an in-depth discussion of the use of standard templates in the context of the FedRAMP program.

5. Threat and vulnerability management;
6. Situational awareness;
7. Information sharing;
8. Workforce and external dependencies management;
9. Incident Response, Monitoring, and Continuity of Operations (COOP) Planning; and,
10. Program management.[7]

For each evaluation domain, IGs would be able to conduct live tests and red-team scenarios across core assets and assess how effectively the processes are managing the performance of information security controls, policies, and processes against the desired risk profile for each asset. For example, IGs might validate asset inventory as a component of the asset, change, and configuration management domain. To assess whether threats are adequately countered, IGs might have the 3PAOs or their equivalent conduct an external penetration test. This assessment process is strongly rooted in each agency's unique risk management attributes and tolerance, as established by IGs and agency leaders. As such, the assessment provides the flexibility to allow for changes in organizational priorities. Moreover, to avoid overemphasizing policy and process in place of systems performance, assessors would regard information security policy and governance processes as foundational criteria for assessing performance within a given risk profile. In these ways, this evaluation process would measure information security risk across key domains according to a specific set of evidence-based criteria.

[7] See Appendix B, "Domains."

Organization Cyber Risk Indicator Determination

By aggregating the results of the information security risk management evaluation, IG evaluations will lead to the identification of a cyber risk indicator for each agency at least once a year. Rather than a subjective grade, this indicator would be a number determined by a formula. It would be used by the agency as well as by oversight entities such as OMB, DHS, GAO, and Congress to improve how risk is managed in an organization.

Much like health care providers measure and report vital signs in a patient, agency CIOs and IGs can assess the basic wellbeing of an organization's risk management policy. These signs will change over time as agency leaders learn more about the relationship between cyber and data protection risks and potential mitigation strategies.

This risk indicator weighs the performance of information systems and the maturity of attendant information security policies and processes according to organizational priorities. This is done to help agencies and departments protect data, serve U.S. citizens, and steward government resources, while enhancing national security. The risk indicator will yield an overall picture of the adequacy of the agency's information security controls in the context of mission priorities. As a part of this process, the recommendations of the IGs should include specific steps for mitigating risks addressed by the indicator's results. It will also allow agencies to measure their progress continuously and plan for improvements in their risk posture.

Agency Continuous Evaluation and Strategic Management Process

Agencies should use the results and findings of the IG process to shape their strategic planning, budgeting, and investment decisions, thereby creating a more integrated operating model.[8] One means by which agencies might gain a more consistent, dynamic sense of how effectively they are managing information security would be to create an

[8] See Julie M. Anderson, A New Operating Model for Government, February 2013, http://www.civitasgroup.com/wp-content/uploads/2013/02/A-New-Operating-Model-for-Government-021913.pdf.

internal dashboard similar to that of the DHS Cyber Scope program that indicates each agency's current cyber risk. CIOs could monitor this dashboard to assess risk on an ongoing basis across an agency's information systems. This dashboard could be refreshed according to an organization's preferences, thus supporting the agency's risk management program to reflect IG findings, changing organization priorities, known vulnerabilities, and risk management milestones. The internal dashboards could also be aggregated across agencies and viewed by DHS to provide a view into known internal and external vulnerabilities for the government as a whole.[9]

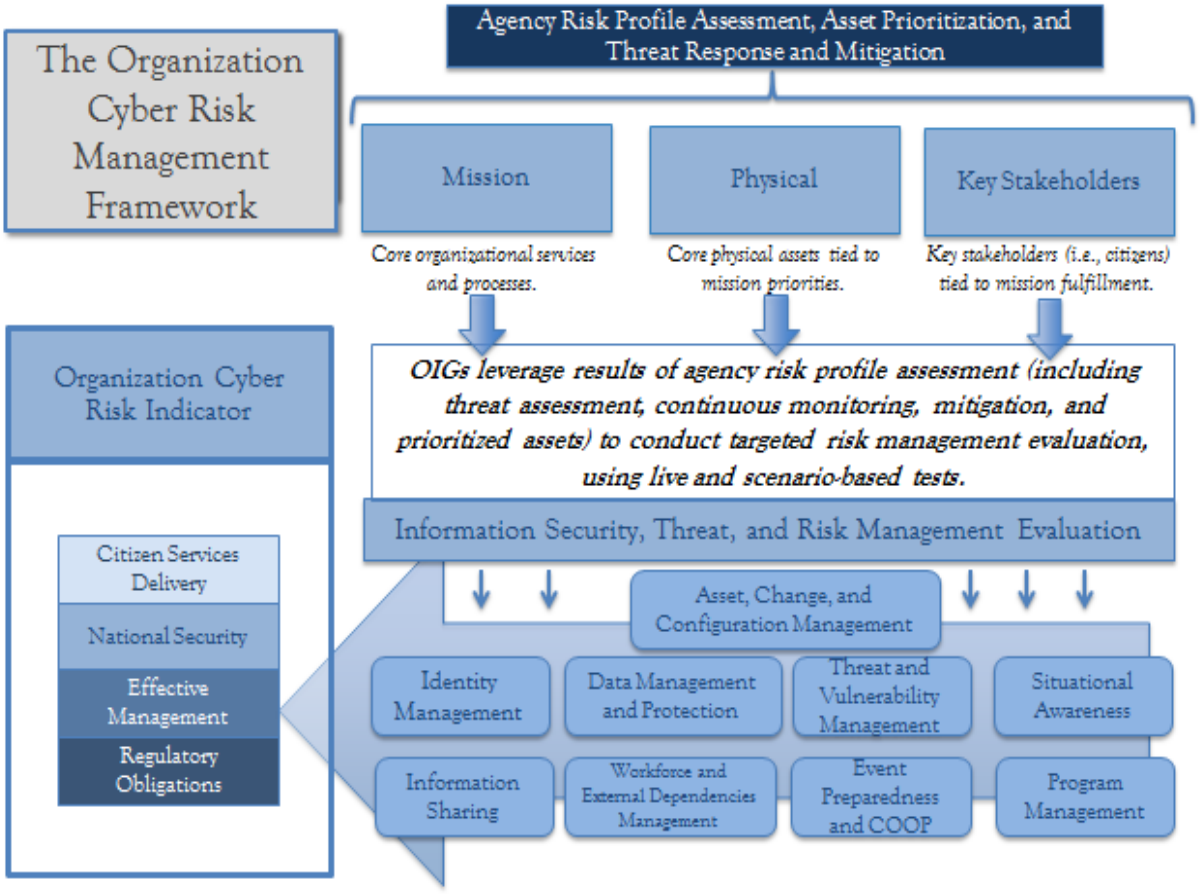

Figure 2. "The Organization Cyber Risk Management Framework."

[9] See Department of Homeland Security, *Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report*, September 2010, http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf.

Benefits of the Framework

By implementing the risk management framework and risk indicator concepts into their operations, government agencies will improve their cybersecurity programs and make the FISMA evaluation process more relevant. The framework helps focus managers' attention by stressing performance outcomes rather than mere compliance, allowing agency leaders to prioritize actions and tie information security investment to overall organizational priorities. Once implemented, the revised evaluation will feed into the risk indicator, providing IGs and agency leaders with a consistent data set and methodology to chart the progress of the agency or department. In essence, the framework provides IGs a better-defined and more integral role in managing the department or agency's information security, while making FISMA's existing guidance regarding risk management more valuable and effective.

Challenges in Implementing a New Approach

In transitioning from the current, compliance-centric system to a more risk management- and outcome-oriented FISMA evaluation process, agency program staff, CIOs, and IGs will undoubtedly face a number of challenges.

First, the framework will require different skillsets from IG and CIO staff. In particular, implementing the framework will require well-trained staff who can disseminate leading practices to help the organizations understand how and why the framework can be effective. Some of the more routine, labor-intensive tasks can be automated, but more skilled workers will be needed for more in-depth technical analysis.

The new approach will also raise questions of cost. With limited resources and growing mandates from Congress, IGs are being asked to do more with less. OMB must offer an explicit tradeoff in its FISMA evaluation guidance about what activities IGs can de-emphasize in order to reallocate resources to implementing the new framework. The report team is convinced that redirecting agency programs from low-payoff cyber tasks will free up the needed resources.

In addition, this transition will require a number of changes to existing guidance and IG FISMA evaluation procedures. Perhaps most notably, it demands a shift in strategic emphasis from complying with annual FISMA guidance to improving how information security risks are managed on a continual, rather than annual, basis. Due to the technical tests of systems performance, IGs are critical to implementing the prioritized, outcome-oriented assessment. The "checklist" approach will help by de-emphasizing basic management processes as minimum requirements for most categories of cyber threat and risk evaluation.

To ensure that the risk management framework and indicator concepts are successfully adopted, OMB must communicate a clear value proposition to the oversight community and agency leaders. In addition to improving the efficacy of the FISMA evaluation process by focusing on priority outcomes, the risk management indicator and its accompanying framework are designed to provide IGs with more explicit, consistent guidance and evaluation tools to improve communications with agency leadership, resolve the identified deficiencies, and acknowledge improvements. The risk management framework continues to uphold and rely on the independence and objectivity of IGs. These values should be communicated explicitly through OMB guidance, as well as through internal department leadership.

Finally, the success of this framework also depends on the ability and willingness of agencies to empower IT leaders in investment and strategic planning decisions. To achieve a closer link between agency investment, planning, and information security risk management, CIOs must be more integrated into department or agency leadership. The ability of agencies to manage risk against known vulnerabilities, while continuing to pursue other agency priorities requires this organizational change.

Policy and guidance should clearly communicate each of these values, as well as identify clear milestones to guide the development and implementation of the technical elements of the framework.

Conclusion

The Federal Information Security Management Act was intended to address and mitigate the cybersecurity threats facing Federal departments and agencies. However, the desired results have not always been achieved. Many current policies and processes guiding the FISMA evaluation process do not substantively contribute to enhancing our government's cybersecurity posture. It is time to redirect scarce Federal resources and revise evaluation methodologies to focus on the dynamic threats that departments and agencies face. To fix the problems of today and those of the years ahead, government should implement a more consistent method of evaluating cybersecurity threats—one which is measurable, transparent, and outcome-oriented. As long as policy guidance falls short and evaluation methods fail to assess which security and data protection mechanisms significantly reduce risk, government will continue to misspend scarce taxpayer resources while failing to address one of the greatest vulnerabilities our nation faces.

Appendix A: Current Environment

Much important work is under way to address the threat. The following list is by no means exhaustive but it is illustrative of efforts that can be leveraged in the further development of this framework.

1. Cross Agency Priority (CAP) Goal of the Administration:
   Cybersecurity is included as one of the fourteen cross-agency priority goals of the Obama Administration and is at the heart of efforts to improve government and protect our national institutions. The purpose of the goals is to improve cross-agency coordination and best practice sharing. The cybersecurity CAP goal focuses on identifying what data and information is entering and exiting their networks, what components are on their information networks, when their security status changes, *and* who is on their systems.

2. Capability Maturity Model Integration (CMMI):
   This model was developed by the Software Engineering Institute (SEI) to address the problems raised by using multiple models of cybersecurity in software and systems development. Originally developed with the intention of evaluating the development and quality of government contractors' software and systems, CMMI has since become the best-known architecture for a maturity model and has been generally applied in other parts of the organization in order to evaluate business processes.

3. The CERT Resilience Management Model (CERT-RMM):
   This model is a capability maturity model for achieving and managing cybersecurity and sustaining businesses. CERT-RMM addresses how cybersecurity is implemented and managed and how businesses are sustained through 26 process areas, each of which addresses a key topic, such as access management or technology management. The 26 process areas in CERT-RMM help an organization:

1. Understand which services are most important to achieving its mission as well as the operational assets (people, information, technologies, and facilities) that are necessary to sustain the delivery of those services; and
2. Develop, operate, and refine protection and sustainment strategies for their most critical assets so that organizational leaders can continue to support the delivery of those services.

4. The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2):
This model allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity, combining elements from existing cybersecurity strategies into a common tool that can be used across the industry. The ES-C2M2 was developed as part of a White House initiative led by DOE in partnership with DHS and involved close collaboration with industry, other Federal agencies, and other stakeholders. The ES-C2M2 was designed specifically for the electric subsector with a Cybersecurity Self Evaluation Survey Tool, which helps electric utilities and grid operators identify opportunities to further develop their own cybersecurity capabilities by posing a series of questions that focus manager's attention on areas such as situational awareness, vulnerabilities, and threat management.

5. Performance Test Scenarios:
The Program Manager for the Information Sharing Environment (PM-ISE)—located within the Office of the Director for National Intelligence—has developed performance test scenarios to translate a strategic objective (e.g., "optimize mission effectiveness") into a realistic illustration. It is intended to describe attributes of an organization by answering questions such as:

- What capability do you want to deliver?
- How do you define success?
- How do you know if you are moving in that direction?
- How do you know *how well* you are progressing?

The performance test scenarios are useful in describing how a highly functioning organization works. By using this type of approach, an agency is able to assess existing capabilities in relationship to where the agency would like to be in the future. The PM-ISE has developed this capability for sharing of terrorism

information. The departments and agencies could utilize a similar methodology in developing their cyber capabilities.

6. Federal Risk Authorization Management Program (FedRAMP):
FedRAMP is the government-wide program managed by GSA that provides a standardized approach for security assessment, authorization, and continuous monitoring for cloud service providers. The program includes testing security controls for FedRAMP security authorization requirements and enables Federal Agencies to use the findings to make risk-based decisions. There are standard templates that provide a consistent method for Third-Party Assessment Organizations (3PAOs) to use when planning to test the security of designated cloud service providers.

   Actual findings from the tests are recorded in FedRAMP security test procedure workbooks and in a Security Assessment Report (SAR). The key improvements which need to continue and be expanded upon include:

   - Establishing technical controls for low and moderate levels process;
   - Using standardized templates;
   - Using independent 3PAOs to ensure the contractors meet the technical controls; and,
   - Maintaining technical controls by conducting quarterly reviews in the actual operating environment.

7. OMB Circular A-123, "Management's Responsibility for Internal Controls:"
The OMB Circular A-123 and the statute it implements, the Federal Managers' Financial Integrity Act of 1982, outline the Federal requirements to improving internal controls and strengthening the requirements for assessing internal controls over financial reporting. It also emphasizes the need for agencies to integrate and coordinate internal control assessments with other internal control-related activities. Within both government and the private sector, leaders must be held accountable, particularly in the area of financial management. Aligning the evaluations with the fiduciary responsibilities will ensure senior management involvement and accountability both within government and with its support contractors.

8. Federal Accounting Standards Advisory Board (FASAB):
   The FASAB serves the public interest by improving federal financial reporting through issuing federal financial accounting standards and providing guidance after considering the needs of external and internal users of federal financial information. By leveraging this existing governance process, this same or a similar board could also establish and agree upon generally accepted security principles which would factor into the overall framework evaluation process.

9. Defense Science Board (DSB) Report on Resilient Military Systems and the Cyber Threat:
   The DSB Task Force Report calls out the need for the Department of Defense to develop the measurement systems necessary to directly determine or predict the resiliency of information systems.

10. Joint Continuous Monitoring Working Group:
    The Joint Continuous Monitoring Working Group was tasked by White House Staff and Federal CIO Council to complete a Concept of Operations for Information Security Continuous Monitoring by April 1, 2013.

Appendix B: Domains

Asset, Change, and Configuration Management:
Asset management is a broad description for activities related to maintaining assets across an enterprise. An asset is anything that has value to an organization, including, but not limited to, another organization, person, computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).[10]

Change Management is a program that describes the procedures necessary to document and ensure systems changes are approved, tested, reviewed and implemented in accordance with the change plan and segregated responsibilities.[11]

Configuration Management is a process for controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation.[12]

Access Management
Access Management is the management of attributes and policies that are used to decide whether a user's request for access to a resource should be granted. In this context, resources can be both computer-based entities (files, Web pages, etc.) and physical entities (buildings, safes, etc.). Users requesting access to resources can be people, processes running on a computer, or devices.[13]

Identity Management
Identity Management is comprised of the set of operations for the life-cycle maintenance of attributes associated with an entity including operations, policies, and technologies, which includes non-human entities and covers identity creation through destruction.[14]

---

[10] David Waltermire, Adam Halbardier, Adam Humenansky, and Peter Mell. "Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains (Draft)," working paper. National Institute of Standards and Technology, 2012. NIST Interagency Report (7800). http://csrc.nist.gov.
[11] Identity Theft Awareness, "NIST Security Compliance." Accessed March 22, 2013. http://www.identity-theft-awareness.com/NIST-security-compliance.html.
[12] Marianne Swanson, Joan Hash, and Pauline Bowen. "Guide for Developing Security Plans for Federal Information Systems." working paper, National Institute of Standards and Technology, 2006. NIST Special Publication (80018) http://csrc.nist.gov.
[13] Nation Institute of Standards and Technology, "A Report on the Privilege (Access) Management Workshop."2010, http://csrc.nist.gov/publications/nistir/ir7657/nistir-7657.pdf.
[14] Information Security and Privacy Advisory Board, "Identity Management Framework." April 2, 2009, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2009-04/ispab_apopowycz_april2009.pdf.

Data Management and Protection
Data Resource Management is the development and execution of architectures, policies, practices and procedures that properly manage the full data lifecycle needs of an enterprise.[15]

Data Protection Management is the administration of backup processes to ensure that tasks run on schedule, and that data is securely backed up and recoverable. Good data protection management means having effective processes and methodologies in place to maintain data integrity.[16]

Threat and Vulnerability Management
Threat and Vulnerability Management provides a way to assess the potential business impact and likelihood of threats and risks to an organization's information infrastructure before those events occur.[17]

Situational Awareness
Situational Awareness describes the ability of an entity to identify, process, and comprehend critical elements of information that may impact an organization's operation or mission. More simply, it means *being aware of what is going on around you.* [18]

Information Sharing
Processes that enable the synthesis and sharing of information and improve collaboration between entities to mitigate cyber threats.[19]

Workforce and External Dependencies Management
Workforce Management is the establishment and maintenance of plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel.[20]

External Dependencies Management is the establishment and maintenance of controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities.[21]

---

[15] Data Management International, "Data Resource Management." 2012. Accessed March 22, 2013. http://www.dama.org/i4a/pages/index.cfm?pageid=3339.
[16] Margaret Rouse. "What is data protection management (DPM)?" 2010. Accessed March 22, 2013. http://searchdatabackup.techtarget.com/definition/data-protection-management-DPM.
[17] John P. Pironti. "Key Elements of a Threat and Vulnerability." Accessed March 22, 2013, http://www.isaca.org/Journal/Past-Issues/2006/Volume-3/Pages/Key-Elements-of-a-Threat-and-Vulnerability-Management-Program1.aspx.
[18] "Situational Awareness." Working paper, Team Coordination Training Student Guide, 1998. http://www.uscg.mil/auxiliary/training/tct/chap5.pdf.
[19] Information Sharing Environment, "Scope of the ISE." Accessed March 22, 2013. http://www.ise.gov/scope-ise.
[20] Department of Energy, *Electricity Subsector Cybersecurity Capability Maturity Model*, 2012. http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model.
[21] Ibid.

Incident Response, Monitoring, and Continuity of Operations (COOP) Planning
Incident Response is the establishment and maintenance of plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event.[22]

Monitoring, or Information Security Continuous Monitoring, is the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[23]

Continuity of Operations (COOP) Planning is a seven-step contingency planning process that an organization may apply to develop and maintain a viable contingency planning program for their information systems.[24]

Program Management
Program Management is the application of knowledge, skills and techniques to execute projects effectively and efficiently. It is a strategic competency for organizations, enabling them to tie project results to business goals and thus better compete in their markets.[25]

[22] Ibid.
[23] Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, and Kevin Stine. "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations." National Institute of Standards and Technology, 2011. NIST Special Publication (800 137), http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.
[24] Marianne Swanson, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, and David Lynes. "Contingency Planning Guide for Federal Information Systems." National Institute of Standards and Technology, 2010. NIST Special Publication (800-34 Rev. 1) http://csrc.nist.gov/rev1_errata-Nov11-2010.pdf.
[25] Project Management Institute, "What is Project Management?" Accessed March 22, 2013. http://www.pmi.org/AboutUs/About-Us-What-is-Project-Management.aspx.

Glossary of Terms

CAP: Cross Agency Priority

CERT-RMM: CERT Resilience Management Model

CIO: Chief Information Officer

CMMI: Capability Maturity Model Integration

COOP: Continuity of Operations Planning

CSIS: Center for Strategic and International Studies

DHS: U.S. Department of Homeland Security

DOE: U.S. Department of Energy

DSB: Defense Science Board

ES-C2M2: Electricity Subsector Cybersecurity Capability Maturity Model

FedRAMP: Federal Risk and Authorization Management Program

FASAB: Federal Accounting Standards Advisory Board

FISMA: Federal Information Security Management Act

GAAP: Generally Accepted Accounting Principles

GAO: U.S. Government Accountability Office

GSA: U.S. General Services Administration

IG: Inspectors General

ISO: International Standards Organization

NIST: National Institute of Standards and Technology

OMB: Office of Management and Budget

PM-ISE: Program Manager for the Information Sharing Environment

POAMS: Plans of Action and Milestones

SAR: Security Assessment Report

SEI: Software Engineering Institute

SP: Special Publication

VA: U.S. Department of Veterans Affairs

3PAO: Third-Party Assessment Organizations

About the Authors

Julie M. Anderson is the COO and a Managing Director at Civitas Group, a strategic advisory services firm in the national security markets. She also serves as an expert for SafeGov.org, an online forum focused on cloud computing policy issues. Recently, Ms. Anderson served as Acting Assistant Secretary for Policy and Planning and Deputy Assistant Secretary for Planning and Evaluation for the U.S. Department of Veterans Affairs (VA) in the Obama Administration. Prior to her appointment, Ms. Anderson worked for IBM's Public Sector Global Business Services practice in Washington, D.C.

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.

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: Technical Proficiency Matters" (CSIS, November 2010) and, with Ms. Evans and others, "Updating U.S. Federal Cybersecurity Policy and Guidance: Spending Scarce Taxpayer Dollars on Security Programs that Work" (CSIS, October 2012).

Meghan M. Wareham is a Senior Associate at Civitas Group where she supports the firm's strategy and M&A investment due diligence practices. In her role, she provides research and analysis for engagements focused on market intelligence, strategy development and business alignment, buy-side M&A strategy, and acquisition due diligence. She has supported numerous engagements across the national security sector with specific areas of focus in defense, intelligence, cybersecurity, and government IT, including the SafeGov.org IT policy initiative.

* Note: Fellow of the National Academy of Public Administration