Submitted by: Nick Marinos, Director, Information Technology & Cybersecurity
SAI USA – U.S. Government Accountability Office (GAO)

Background

Since the early 1990s, our high-risk program has focused attention on government operations with greater vulnerabilities to fraud, waste, abuse, and mismanagement; or that are in need of transformation to address economy, efficiency, or effectiveness challenges. The cornerstone of this program is the High-Risk Report, which we issue on a biennial basis, based on an analysis of our entire body of work. To determine which federal government programs and functions should be designated high-risk, we consider qualitative factors, such as whether the risk:

* involves public health or safety, service delivery, national security, national defense, economic growth, or privacy or citizens’ rights, or
* could result in significantly impaired service, program failure, injury or loss of life, or significantly reduced economy, efficiency, or effectiveness.

We also consider the exposure to loss in monetary or other quantitative terms. At a minimum, $1 billion must be at risk, in areas such as:

* the value of major assets being impaired;
* revenue sources not being realized;
* major agency assets being lost, stolen, damaged, wasted, or underutilized; potential for, or evidence of improper payments; and
* presence of contingencies or potential liabilities. Before making a high-risk designation, we also consider corrective measures planned or under way to resolve a material control weakness and the status and effectiveness of these actions.

This effort, supported by the U.S. Senate Committee on Homeland Security and Governmental Affairs and by the U.S. House of Representatives Committee on Oversight and Reform, has brought much needed attention to problems impeding effective government and costing billions of dollars each year.

Our most recently issued 2019 report[[1]](#footnote-1) reviewed the status of 35 high-risk areas on the list and outlined steps to lasting solutions. Among the areas highlighted within this report was the call for “Ensuring the Cybersecurity of the Nation”.

High-Risk Area: Ensuring the Cybersecurity of the Nation.

Federal agencies and the nation’s critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being. The risks to systems underpinning the nation’s critical infrastructure are increasing as security threats evolve and become more sophisticated.

We first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015. In 2018, we updated this high-risk area to reflect the lack of a comprehensive cybersecurity strategy for the federal government.

Since 2010, we have made over 3,000 recommendations to federal agencies aimed at addressing cybersecurity shortcomings, including protecting cyber critical infrastructure, managing the cybersecurity workforce, and responding to cybersecurity incidents. Of those 3,000 recommendations, 448 were made since our last high-risk update in February 2017. Although many recommendations have been addressed, about 700 have not yet been implemented.

High-Risk List: Key Elements Needed to Make Progress Toward High-Risk Area Removal

Our experience has shown that the key elements needed to make progress toward being removed from the High-Risk List are top-level attention by the administration and agency leaders grounded in the five criteria for removal, as well as any needed congressional action. The five criteria for removal that we identified in November 2000 are as follows:

* **Leadership Commitment.** Demonstrated strong commitment and top leadership support.
* **Capacity.** The agency has the capacity (i.e., people and resources) to resolve the risk(s).
* **Action Plan.** A corrective action plan exists that defines the root cause, solutions, and provides for substantially completing corrective measures, including steps necessary to implement solutions we recommended.
* **Monitoring.** A program has been instituted to monitor and independently validate the effectiveness and sustainability of corrective measures.
* **Demonstrated Progress.** Ability to demonstrate progress in implementing corrective measures and in resolving the high-risk area.

These five criteria form a road map for efforts to improve and ultimately address high-risk issues. Addressing some of the criteria leads to progress, while satisfying all of the criteria is central to removal from the list. Importantly, the actions listed are not “stand alone” efforts taken in isolation from other actions to address high-risk issues. That is, actions taken under one criterion may be important to meeting other criteria as well. For example, top leadership can demonstrate its commitment by establishing a corrective action plan including long-term priorities and goals to address the high-risk issue and using data to gauge progress—actions which are also vital to monitoring criteria.

History of the Cybersecurity High-Risk Area

Between 1993 and 1997, we issued over 30 reports describing serious information security weaknesses at major U.S. federal agencies. For example:

* In May 1996, we reported that tests at the Department of Defense showed that Defense systems may have experienced as many as 250,000 attacks during 1995, that about 64 percent of attacks were successful at gaining access, and that only a small percentage of these attacks were detected.
* Many of the federal information security weaknesses and causal factors reported over those years were identified as a direct result of the annual financial statement audits initiated under the Chief Financial Officers Act of 1990. Although these audits pertained primarily to financial management systems, they generally included a review of computer-based controls that affected a significant portion of an agency’s broader operations.

**GAO’s Early Work Led to the Information Security High-Risk Designation in 1997**

When introducing information security to the High-Risk list in 1997, we pointed out several related problems that needed to be addressed to help ensure that federal agencies adequately protected their systems and data. These included:

* insufficient awareness and understanding of information security risks among senior agency officials,;
* poorly designed and implemented security programs that do not adequately monitor controls or proactively address risk; and
* a shortage of personnel with the training and technical expertise needed to manage security controls in today’s sophisticated information technology environment.

Following the high-risk designation, we issued several products aimed at improving the guidance and resources available to federal agency officials in ensuring the effectiveness of information security programs.

**GAO Added Critical Infrastructure Cybersecurity to the High-Risk Area in 2003**

In our January 2001 high-risk update report, we began to highlight the increasing importance of the federal government’s efforts to protect our nation’s critical public and private computer-dependent infrastructure.

In our 2003 high-risk update report, we broadened the information security high-risk area to include cyber critical infrastructure protection (CIP), noting that, although the federal government had made steady progress in working with the private sector to better secure critical infrastructures, this issue should be designated as part of our information security high-risk issue because:

* failure to adequately protect these infrastructures could have consequences for national security, national economic security, and/or national public health and safety;
* terrorist groups and others have stated their intentions of attacking our critical infrastructures;
* federal influence over the private sector’s management of our nation’s critical infrastructures poses unique challenges; and
* further actions on GAO’s CIP recommendations were needed, including (1) developing a national CIP strategy, (2) improving analysis and warning capabilities, and (3) improving information sharing on threats and vulnerabilities.

**Protecting the Privacy of PII Was an Important Addition to the High-Risk Area in 2015**

In our 2015 high-risk update report, we noted that advancements in technology had made it easier for individuals and organizations to correlate data and track it across large and numerous databases. Furthermore, the number of reported security incidents involving personally identifiable information (PII) at federal agencies had increased significantly in recent years and a number of high-profile breaches of PII had occurred at commercial entities.

In the lead up to the high-risk area expansion, we issued several reports on the topic of privacy and data protection. For example:

* In July 2012, we testified that technological developments since major U.S. privacy legislation became law in 1974 had rendered some of the provisions within it and other related laws inadequate to fully protect all PII collected, used, and maintained by the federal government.
* In September 2013, we noted that no overarching federal privacy law governed the collection and sale of personal information among private sector companies, including information resellers (companies that collect and resell information on individuals.

2018 Mid-Cycle Update: Ensuring the Cybersecurity of the Nation

At the direction of the U.S. Comptroller General, we initiated an update to the information security high-risk area in advance of the planned 2019 update of the entire High-Risk report. This report[[2]](#footnote-2) was issued in September 2018 and was aimed at providing an “off cycle” review of the cybersecurity high-risk area in order to identify actions that the federal government and other entities need to take to address cybersecurity challenges facing the nation.

In conducting the work for this update, we first identified cybersecurity areas in which the federal government has experienced challenges. To do so, we primarily reviewed our prior work issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity incidents, among other areas. We also reviewed recent cybersecurity policy and strategy documents issued by the current administration. We then analyzed these documents to determine the extent to which they included GAO’s desirable characteristics of a national strategy. We also reviewed recent media and information security industry reports of cyberattacks and security breaches.

Based on these actions, we identified four cybersecurity areas in which federal agencies had experienced challenges. These included (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data. To address these challenges, we identified 10 critical actions that the federal government and other entities need to take (see figure 1 below). In addition, we also discussed in more detail each of the 10 actions in appendices at the end of the report.

**Figure 1: Ten Critical Actions Needed to Address Four Major Cybersecurity Challenges**



These 10 action areas were a reflection of the work we performed across dozens of audits and evaluations. Since 2010, we have made over 3,000 recommendations to agencies through these reports aimed at addressing cybersecurity challenges facing the government—448 of which were made since the last high-risk update in February 2017. Nevertheless, many agencies face challenges in safeguarding their information systems and information, in part because many of these recommendations have not been fully implemented. Of the roughly 3,000 recommendations made since 2010, nearly 700 had not been fully implemented as of December 2018. We have also designated 35 as priority recommendations, meaning that we believe these recommendations warrant priority attention from heads of key departments and agencies. As of December 2018, 26 of our priority recommendations had not been fully implemented.

Action #1: Develop and Execute a More Comprehensive Strategy for National Cybersecurity and Global Cyberspace

Federal law and policy call for a risk-based approach to managing cybersecurity within the government, as well as globally.[[3]](#footnote-3) We have previously reported that the federal government has faced challenges in establishing a comprehensive strategy to provide a framework for how the United States will engage both domestically and internationally on cybersecurity-related matters.

More specifically, in February 2013, we reported that the government had issued a variety of strategy-related documents that addressed priorities for enhancing cybersecurity within the federal government as well as for encouraging improvements in the cybersecurity of critical infrastructure within the private sector; however, no overarching cybersecurity strategy had been developed that articulated priority actions, assigned responsibilities for performing them, and set time frames for their completion.[[4]](#footnote-4) Accordingly, we recommended that the White House Cybersecurity Coordinator[[5]](#footnote-5), in the Executive Office of the President, develop an overarching federal cybersecurity strategy that included all key elements of the desirable characteristics of a national strategy[[6]](#footnote-6) including, among other things, milestones and performance measures for major activities to address stated priorities; cost and resources needed to accomplish stated priorities; and specific roles and responsibilities of federal organizations related to the strategy’s stated priorities.

In response to our recommendation, in October 2015, the Director of OMB and the Federal Chief Information Officer, issued a *Cybersecurity Strategy and Implementation Plan* for the federal civilian government. The plan directed a series of actions to improve capabilities for identifying and detecting vulnerabilities and threats, enhance protections of government assets and information, and further develop robust response and recovery capabilities to ensure readiness and resilience when incidents inevitably occur. The plan also identified key milestones for major activities, resources needed to accomplish milestones, and specific roles and responsibilities of federal organizations related to the strategy’s milestones.

Since that time, the executive branch has made progress toward outlining a federal strategy for confronting cyber threats. Our September 2018 off-cycle report and March 2019 High Risk report highlighted a variety of efforts and assessed them based on this set criteria. We noted that these efforts provide a good foundation toward establishing a more comprehensive strategy, but additional effort is needed to address all of the desirable characteristics of a national strategy that we recommended. We stated that recently issued executive branch strategy documents did not include key elements of desirable characteristics that can enhance the usefulness of a national strategy as guidance for decision makers in allocating resources, defining policies, and helping to ensure accountability. Specifically:

* Milestones and performance measures to gauge results were generally not included in strategy documents. Without such performance measures, federal agencies will lack a means to ensure that the goals and objectives discussed in the document are accomplished and that responsible parties are held accountable.
* Strategy documents generally did not include information regarding the resources needed to carry out the goals and objectives. Without information on the specific resources needed, federal agencies may not be positioned to allocate such resources and investments and, therefore, may be hindered in their ability meet national priorities.
* Most of the strategy documents lacked clearly defined roles and responsibilities for key agencies, especially those that contribute substantially to the nation’s cybersecurity programs. Without this information, the federal government may not be able foster effective coordination, particularly where there is overlap in responsibilities, or hold agencies accountable for carrying out planned activities.

Ultimately, a more clearly defined, coordinated, and comprehensive approach to planning and executing an overall strategy would likely lead to significant progress in furthering strategic goals and lessening persistent weaknesses.

What’s Next for the High-Risk Area

The cybersecurity high-risk area serves dual purposes. It not only helps inform Congress and the public about the urgent actions needed to address the nation’s cybersecurity challenges, but also provides a roadmap for ongoing and future GAO reviews. We routinely rely on the structure of the high-risk area (4 challenges, 10 actions) in developing our audit portfolio and working with members of Congress and their staff in setting priorities for oversight activities and areas of needed focus. We also recently initiated a review of cybersecurity leadership and strategy across the U.S. federal government. As part of that review, we are evaluating what additional steps are necessary for the federal government to take in developing and executing a more comprehensive strategy for dealing with cyber threats. We intend to complete that work in calendar year 2019 to help inform future updates to the cybersecurity high-risk area in calendar year 2020-21.

1. GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019). [↑](#footnote-ref-1)
2. *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*. [GAO-18-622](https://www.gao.gov/products/GAO-18-622). Washington, D.C.: September 6, 2018. [↑](#footnote-ref-2)
3. This includes the Federal Information Security Modernization Act of 2014, Revision of the Office of Management and Budget’s Circular No. A-130, “*Managing Information as a Strategic Resource*” and Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. [↑](#footnote-ref-3)
4. *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented.* GAO-13-187. Washington, D.C.: February 14, 2014. [↑](#footnote-ref-4)
5. In December 2009, a Special Assistant to the President was appointed as Cybersecurity Coordinator to address the recommendations made in the Cyberspace Policy Review, including coordinating interagency cybersecurity policies and strategies and developing a comprehensive national strategy to secure the nation’s digital infrastructure. [↑](#footnote-ref-5)
6. In 2004, we developed a set of desirable characteristics that can enhance the usefulness of national strategies in allocating resources, defining policies, and helping to ensure accountability. (GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004)). [↑](#footnote-ref-6)