United States Government Accountability Office

GAO

Report to Congressional Requesters

January 2013

INFORMATION SECURITY

Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project

GAO-13-155

January 2013

INFORMATION SECURITY

Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-155, a report to congressional requesters

Why GAO Did This Study

In September 2011, FCC discovered that it had experienced a security breach on its computer network, which potentially allowed sensitive information to be compromised. The commission initiated the ESN project to implement enhanced security controls and an improved network architecture to defend against cyber attacks and reduce the risk of a successful future attack.

GAO was asked to assess the extent to which FCC has (1) effectively implemented appropriate information security controls for the initial components of the ESN project, and (2) implemented appropriate procedures to manage and oversee its ESN project.

To do so, GAO determined the effectiveness of ESN security controls by evaluating control configurations and identifying management controls; and determined how FCC applied them to the ESN project by analyzing documentation and interviewing commission officials.

What GAO Recommends

GAO is making seven recommendations to the FCC to implement management controls to help ensure that ESN meets its objective of securing FCC's systems and information. In commenting on a draft of this report, FCC concurred with the recommendations. In a separate report with limited distribution, GAO is also making 26 recommendations to resolve technical information security weaknesses related to access controls and configuration management of the ESN.

View GAO-13-155. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, Valerie Melvin at (202) 512-6304 or melvinv@gao.gov, and Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The Federal Communications Commission (FCC) did not effectively implement appropriate information security controls in the initial components of the Enhanced Secured Network (ESN) project. Although FCC took steps to enhance its ability to control and monitor its network for security threats, weaknesses identified in the commission's deployment of components of the ESN project as of August 2012 resulted in unnecessary risk that sensitive information could be disclosed, modified, or obtained without authorization. This occurred, in part, because FCC did not fully implement key information security activities during the development and deployment of the initial components of the project. While FCC policy is to integrate security risk management into system life-cycle management activities, the commission instead deployed the initial components of the ESN project without, among other things, first selecting and documenting the security controls, assessing the controls, or authorizing the system to operate. As a result of these deficiencies, FCC's information remained at unnecessary risk of inadvertent or deliberate misuse, improper disclosure, or destruction. Further, addressing these deficiencies could require costly and time-consuming rework.

FCC's efforts to effectively manage the ESN project were hindered by its inconsistent implementation of procedures for estimating costs, developing and maintaining an integrated schedule, managing project risks, and conducting oversight. If not addressed, these weaknesses could pose challenges for the commission to achieve the project's goal of improved security. Specifically, FCC

- had not developed a reliable life cycle cost estimate for ESN that includes all implementation costs;
- did not, in its project schedule, adequately identify the sequence in which activities must occur, ensure that detailed activities were traceable to higher-level activities, or establish a baseline schedule;
- documented and managed some risks to project success, but its prime contractor did not identify any project risks until after the deployment of the initial components of the ESN project had begun; and
- had not included the ESN project in its processes for conducting regular oversight of information technology projects.

According to FCC officials, a key reason that they had not fully applied their policies or widely accepted best practices for security risk management and project management is because the ESN project was an emergency project and, therefore, needed to be initiated quickly. However, while GAO agrees that the security threat makes implementation urgent, it does not negate the need to perform key security risk management activities. Unless FCC more effectively implements its IT security policies and improves its project management practices and effectively applies them to the ESN project, unnecessary risk exists that the project may not succeed in its purpose of effectively protecting the commission's systems and information.

Contents

Letter		1
	Background	3
	FCC Did Not Effectively Implement Appropriate Information Security Controls in the Initial Components of Enhanced Secured Network Project	9
	FCC Has Not Consistently Implemented Key Procedures for Managing the Enhanced Secured Network Project	14
	Conclusions	19
	Recommendations for Executive Action	20
	Agency Comments	21
Appendix I	Objectives, Scope, and Methodology	23
Appendix II	Comments from the Federal Communications Commission	26
Appendix III	GAO Contacts and Staff Acknowledgments	30

Figures

Figure 1: Timeline of the ESN Project	8
Figure 2: FCC Life-cycle Integrating Security Risk Management and Life-cycle Management	12

Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMMI®	Capability Maturity Model® Integration
ESN	Enhanced Secured Network
FCC	Federal Communications Commission
IT	information technology
NIST	National Institute of Standards and Technology
SP	Special Publication

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 25, 2013

The Honorable Chairman
The Honorable Ranking Member
Subcommittee on Financial Services
and General Government
Committee on Appropriations
United States Senate

The Honorable Ander Crenshaw
Chairman
The Honorable Jose E. Serrano
Ranking Member
Subcommittee on Financial Services
and General Government
Committee on Appropriations
House of Representatives

Cyber-based threats to federal information systems are evolving and growing. These threats can be intentional or unintentional and can come from a variety of sources, including criminals, foreign nations, terrorists, and other adversarial groups. Further, the growing interconnectivity among different types of information systems presents increasing opportunities for such attacks. Given the increasing number of reported information security incidents, coupled with the advancement of security attacks, federal agencies' information and information systems remain at risk.

In September 2011, the Federal Communications Commission (FCC) discovered a cybersecurity incident and took action to identify and remove infected workstations and identify significant factors that increased risk to its network. The commission initiated the Enhanced Secured Network (ESN) project to improve its computer security by implementing enhanced security controls to defend against cyber attacks. To execute this project, in November 2011, FCC requested and received approval from the Office of Management and Budget to use $10 million in previously de-obligated funds and gained congressional agreement with the reprogramming plan in December 2011.

In view of the importance of the actions that FCC is taking to implement enhanced security controls over its computerized systems and information, you asked us to assess the extent to which FCC has (1)

effectively implemented appropriate information security controls for the initial components of its ESN project; and (2) implemented appropriate procedures to manage and oversee its ESN project.

To assess FCC's implementation of security controls for the deployment of initial components of the ESN, we examined the information security controls at FCC and compared them to relevant guidance issued by the National Institute of Standards and Technology (NIST) to determine whether resources and information were adequately protected from unauthorized use, fraudulent use, disclosure, or destruction. We concentrated our evaluation on security controls implemented as of August 2012. In addition, we examined FCC policies and project documentation and interviewed FCC officials to evaluate the commission's policies and practices in the areas of security risk management and life-cycle management.

To assess FCC's procedures to manage and oversee the project, we evaluated key areas of information technology (IT) project management: cost estimation, scheduling, project risk management, and investment management. For each of these areas, we determined how FCC applied them to the ESN project by analyzing pertinent documentation—such as agency policies, procedures, plans, meeting minutes, e-mails, and risk logs—and by interviewing agency officials. We compared the information collected to relevant guidance from the Office of Management and Budget and to widely accepted practices for system development and acquisition, cost and schedule estimating, and IT investment management such as the Software Engineering Institute's[1] Capability Maturity Model® Integration for Development[2] and CMMI® for Acquisition;[3] and GAO's

[1]The Software Engineering Institute is a federally funded research and development center whose mission is to advance software engineering and related disciplines to ensure the development and operation of systems with predictable and improved cost, schedule, and quality.

[2]Software Engineering Institute, *CMMI® for Development*, Version 1.3 (Pittsburgh, Pa.: November 2010).

[3]Software Engineering Institute, *CMMI® for Acquisition*, Version 1.3 (Pittsburgh, Pa.: November 2010).

Cost Estimating and Assessment Guide,[4] Schedule Assessment Guide,[5] and Information Technology Investment Management framework.[6]

We conducted this performance audit from May 2012 to January 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Further details of our objectives, scope, and methodology are contained in appendix I.

Background

Established by the Communications Act of 1934,[7] FCC regulates interstate and international communications by radio, television, wire, satellite, and cable. It is responsible for, among other things, making available rapid, efficient, nationwide, and worldwide wire and radio communication services at reasonable charges and on a nondiscriminatory basis, and more recently, promoting competition and reducing regulation of the telecommunications industry in order to secure lower prices and higher quality services for consumers.[8]

FCC is charged with carrying out various activities, including issuing licenses for broadcast television and radio; overseeing licensing, enforcement, and regulatory functions of carriers of cellular phones and other personal communication services; regulating the use of radio spectrum and conducting auctions of licenses for spectrum; investigating complaints and taking enforcement actions if it finds that there have been violations of the various communications laws and commission rules that

[4]GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009).

[5]GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules (Exposure Draft)*, GAO-12-120G (Washington, D.C.: May 2012).

[6]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004).

[7]47 U.S.C. § 151.

[8]The Telecommunications Act, which substantially amended the Communications Act, effected comprehensive reform of the nation's telecommunications statutory and regulatory framework. Pub. L. No. 104-104, 110 Stat. 56 (1996).

are designed to protect consumers; addressing public safety, homeland security, emergency management, and preparedness; educating and informing consumers about communications goods and services; and reviewing mergers of companies holding FCC-issued licenses.

FCC's basic structure is prescribed by statute. It is composed of five commissioners, appointed by the President with the advice and consent of the Senate to serve 5-year terms. No more than three commissioners may come from any one political party.[9] The President designates one of the commissioners as chairman. The chairman derives authority from the provisions of the Communications Act and FCC rules which define the chairman's duties to include, among other things, presiding at all meetings and sessions of the commission, representing the commission in all matters relating to legislation and before other government offices, and generally organizing and coordinating the work of the commission. The commissioners delegate many of FCC's day-to-day responsibilities to the commission's 7 bureaus and 10 offices. The chairman also delegates management and administrative responsibilities, including IT, to FCC's Office of the Managing Director.

The FCC relies extensively on computerized systems to support its mission-related operations in addition to information security controls to protect agency data. The use of IT to implement the commission's business operations is performed by FCC's Information Technology Center which is organizationally placed within the Office of the Managing Director. Through its computer network and systems, the FCC collects and maintains non-public information, including proprietary information of businesses regulated by the commission.

In an effort to meet federal information security requirements and address implementing guidance, the Managing Director established a cybersecurity program and delegated key information security responsibilities to the commission's Chief Information Officer (CIO). The CIO is responsible for, among other things:

- overseeing the development and maintenance of the cybersecurity program;

[9]47 U.S.C. § 154.

- designating and assigning responsibility to the FCC's Chief Information Security Officer (CISO) for managing the program;
- coordinating with the Managing Director to ensure provision of adequate budget, staffing, and training resources required to implement the program; and
- evaluating and approving CISO-recommended resolution of issues related to cybersecurity.

FCC and the Federal Government Face Cybersecurity Threats

Information security is critical for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, such as the FCC, where maintaining the public's trust is essential. While the use of interconnected electronic information systems allows FCC to accomplish its mission more quickly and effectively, their use also poses significant risks to the commission's computer systems and to the critical operations they support.

We have previously reported on the increasing number of cybersecurity attacks affecting federal information systems.[10] Consistent with this, reports of security incidents from federal agencies are on the rise. Federal agencies have reported increasing numbers of security incidents that placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. Over the past 6 years, the number of incidents reported by federal agencies to the United States Computer Emergency Readiness Team[11] increased from 5,503 incidents in fiscal year 2006 to 48,563 incidents in fiscal year 2012, an increase of more than 780 percent. Accordingly, we have designated information security

[10]GAO, *Cybersecurity: Threats Impacting the Nation*, GAO-12-666T (Washington, D.C.: Apr. 24, 2012).

[11]The Department of Homeland Security's federal information security incident center is hosted by United States Computer Emergency Readiness Team. When incidents occur, agencies are to notify the center.

as a governmentwide high risk area since 1997, a designation that remains in force today.[12]

Without proper safeguards, systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

FCC Initiated the Enhanced Secured Network Project in Response to Security Breach

In September 2011, the FCC discovered that it had suffered a security breach on its agency network. FCC's actions to respond to the incident included, among other things, identifying and removing infected workstations and identifying significant factors that increased risk to its network. FCC initiated the ESN project in order to continue its response to the incident, mitigate the risk to its information resources from the malicious software, reduce the risk of a successful future attack, and address weaknesses in its security controls and network architecture. To execute this project, in November 2011, FCC requested and received approval from the Office of Management and Budget to use $10 million in previously deobligated funds and gained congressional agreement with the reprogramming plan in December 2011, contingent upon the commission providing Congress with quarterly briefings on the project's status until completion.

The ESN project includes two major efforts: (1) implementing enhanced security controls, and (2) designing and implementing a sustainable cyber threat analysis and mitigation program.

- *Enhanced security controls.* The project is intended to enhance and augment FCC's existing security controls through changes to the network architecture and by implementing, among other things, additional intrusion detection tools, network firewalls, and audit and monitoring tools.

- *Cyber threat analysis and mitigation.* In addition to enhancing security controls, the ESN project aims to develop a sustainable cyber threat analysis and mitigation program that is to include risk management

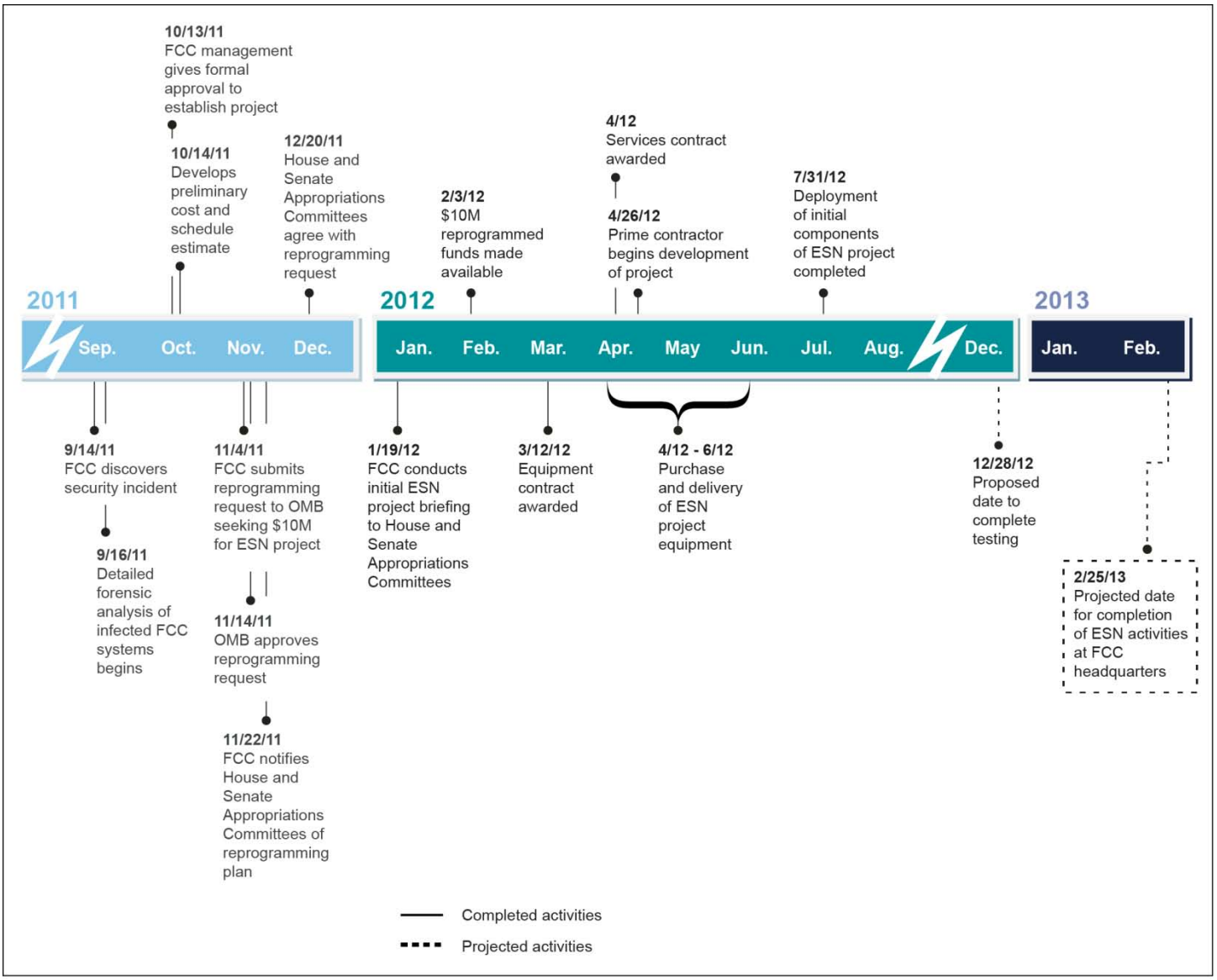
[12]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

guidelines for assessing security threats and subsequent mitigation strategies. This effort is intended to provide FCC with mechanisms to analyze the criticality of commission assets, assess the likelihood that threats will endanger assets, and identify actions to reduce those risks and mitigate the consequences of an attack.

In January 2012, FCC officials briefed congressional staff on its development plans for the ESN project, including, among other things, the planned schedule for acquiring and implementing new hardware and enhanced security controls and for instituting a cyber threat analysis and mitigation program in multiple phases over a 1-year period, from February 1, 2012, to January 31, 2013. The reprogrammed funds were made available for the project in February 2012, and FCC subsequently purchased equipment and engaged a prime contractor for the project in April 2012. FCC entered the project's system development phase in April 2012, received final delivery of hardware in June 2012, and deployed the initial components of the project by the end of July 2012. This included making changes to the network architecture to enhance protection for an initial portion of the commission's executives and their key staff. Officials stated that activities to deploy enhanced protections for all users at FCC headquarters are projected to be completed in February 2013, and that these protections will be expanded to the commission's field offices at a later date.

To protect against and detect cyber attacks, FCC also deployed a malware protection system for its network and a tool to monitor its workstations for signs of compromise. Figure 1 depicts the project timeline from the discovery of the security incident through the projected date of completion for the ESN project.

Figure 1: Timeline of the ESN Project



Source: GAO analysis of FCC information.

FCC Did Not Effectively Implement Appropriate Information Security Controls in the Initial Components of Enhanced Secured Network Project

FCC did not effectively implement appropriate information security controls in the initial components of the ESN project. Although the commission deployed enhanced security controls and tools for monitoring and controlling security threats as of August 2012, it had not securely configured these tools and other network devices to sufficiently protect the confidentiality, integrity, and availability of its sensitive information. These weaknesses occurred, at least in part, because FCC did not fully perform key security risk management activities during the development and deployment of the ESN project. As a result, FCC limited the effectiveness of its security enhancements and its sensitive information remained at unnecessary risk of inadvertent or deliberate misuse, improper disclosure, or destruction.

Initial Components of Enhanced Secured Network Project Were Deployed With Significant Security Weaknesses

A basic management objective for any organization is to protect confidentiality, integrity, and availability of the information and systems that support its critical operations and assets. Organizations accomplish this by designing and implementing access and other controls that are intended to protect information and systems from unauthorized disclosure, modification, and loss. Specific controls include, among other things, those related to system boundary protections, identification and authentication of users, authorization restrictions, cryptography, audit and monitoring procedures, and configuration management. NIST guidance recommends, among other things, that organizations should (1) control and regulate the information transmitted between interconnected systems; (2) ensure that passwords are encrypted while being stored; and (3) employ tools and techniques to monitor events on information systems, detect attacks, and provide identification of unauthorized use of systems.

The initial components of the project included making changes to the network architecture to better protect the commission's executives and their key staff. In addition, the commission deployed a malware protection system on its network and a tool to monitor its workstations for signs of compromise.

However, FCC did not effectively implement or securely configure key security tools and devices to protect these users and its information against cyber attacks. For example:

- Certain boundary protection controls were configured in a manner that limited the effectiveness of network monitoring controls.

- Stored passwords were not always strongly encrypted on network devices.

- Although a malware protection tool had been implemented to detect and prevent cyber attacks, the tool's capabilities for preventing certain attacks were not fully implemented.

As a result of these and other deficiencies, FCC faces an unnecessary risk that individuals could gain unauthorized access to its sensitive systems and information.

In addition to the above deficiencies, we identified other security weaknesses in controls related to boundary protection, identification and authentication, authorization, cryptography, audit and monitoring, and configuration management that limit the effectiveness of the security enhancements and unnecessarily place sensitive information at risk of unauthorized disclosure, modification, or exfiltration. The control weaknesses we identified during this review are described in a separate report with limited distribution.

FCC Did Not Fully Implement Key Risk Management Activities in Developing and Deploying the Initial Components of the Enhanced Secured Network Project

The information security weaknesses in the initial portions of the project occurred, in part, because FCC had not fully performed key information security activities during the development and deployment of these initial components. Although FCC's life-cycle management policy integrates information security risk management activities into its life-cycle management processes—such as selecting and documenting security controls during the requirements and design life-cycle phase—it did not fully implement its policies on the ESN project. Instead, FCC deployed the initial components of the project without first fully defining security and functional requirements and without conducting required reviews of those requirements.

Federal Guidelines and FCC Policy Require Integration of Information Security Risk Management Activities throughout the Life Cycle

According to NIST, the most effective method for ensuring that an organization's protection strategy is implemented is to integrate information security into the system life cycle from inception. NIST has specified a risk management framework to guide agencies in integrating security risk management activities into agency life-cycle processes.[13] Among other things, the framework emphasizes that agencies should (1) select security controls and document the controls in the system security plan;[14] (2) assess the implementation of the controls to determine the extent to which they are implemented correctly, are operating as intended, and meet the security requirements; and (3) authorize the system to operate based on the results of security assessments and a determination of risk.

To the commission's credit, FCC's life-cycle management and cybersecurity policies integrate security risk management activities into the life cycle. Specifically, FCC's life-cycle management policy states that security controls should be selected and documented during the requirements and design life cycle phase. Additionally, it states that security controls should be implemented and assessed during the development and test life-cycle phase. Further, the cybersecurity policy states that systems should be authorized to operate, during the development and test life-cycle phase, prior to being deployed to production. Lastly, the policy states that re-authorization must occur prior to a significant change to the information system or at least every 3 years.

Consistent with best practices for system acquisition,[15] the commission's life-cycle management policy also documents dependencies among life-cycle activities. For example, it states that security and functional requirements should be developed prior to designing the system and selecting the security controls, which, in turn, should be completed prior to moving ahead with building the system and implementing the security

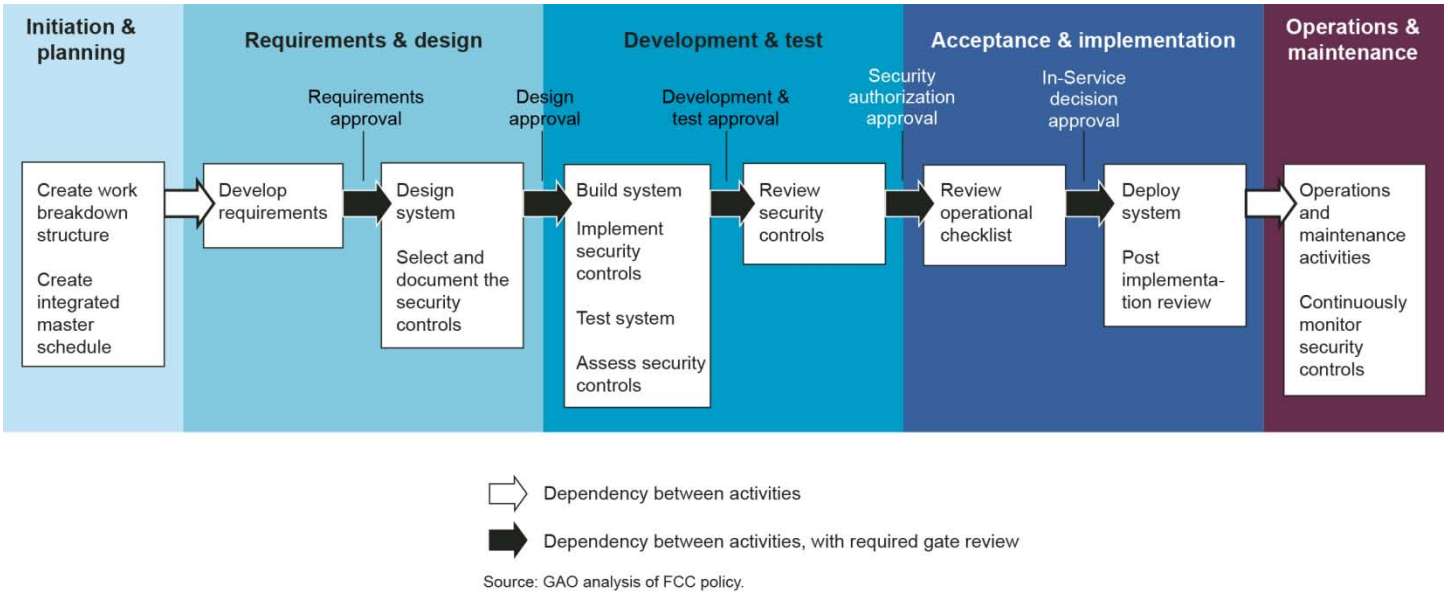
[13]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37 Revision 1 (Gaithersburg, Md.: February 2010).

[14]Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. An example of a security control is establishing a policy that passwords be changed every 90 days.

[15]SEI, CMMI® for Acquisition.

controls. Further, the policy calls for technical reviews, in the form of "gate" reviews, to be conducted throughout the life cycle at major transition points between key activities, such as a Requirements Approval prior to design and development activities and an In-Service Decision Approval prior to deployment, to ensure that a formal decision is made to approve the execution of further activities. Figure 2 illustrates FCC's life-cycle management process.

Figure 2: FCC Life-cycle Integrating Security Risk Management and Life-cycle Management



Source: GAO analysis of FCC policy.

FCC Did Not Fully Perform Key Security Risk Management Activities in Developing and Deploying the Initial Components of the Enhanced Secured Network Project

FCC did not fully perform key information security risk management activities called for within its own policies during the development and deployment of the initial components of the project. Specifically:

- **Selecting and documenting security controls:** At the time that the enhanced security controls were deployed in July 2012, FCC had not fully developed their security requirements. Draft requirements had been developed; however, many of them—including security requirements—lacked details or contained placeholders for more information. For example, a high-priority requirement for boundary protection contained only placeholders for information regarding the network configuration needed to implement this control.

- **Assessing security controls:** Although FCC implemented certain security tools and hardware, the commission did not effectively

assess the implementation of these security controls to determine the extent to which they were implemented correctly, operating as intended, and met security requirements prior to deploying them to protect key users and commission information. Officials stated that they verified the functional configuration of user workstations and ensured that users could access network resources and local applications; however, the security controls were not specifically tested.

- **Authorizing the system:** FCC did not reauthorize the general support system to operate prior to deployment. Although FCC's cybersecurity policy requires that systems be reauthorized prior to a significant change to the system, the FCC general support system—which includes the initial components of the ESN project—had not been reauthorized since May 2011, 14 months before the initial deployment.

In deploying the initial components of the project, FCC also did not perform key life-cycle activities in accordance with the dependencies and gate reviews documented in its life-cycle policy. In particular, although FCC had planned to complete the development of security and functional requirements and hold a requirements review in June 2012, the commission proceeded with deployment without completing these activities. In a recent draft project schedule, the commission indicated that it intends to complete these activities in December 2012.

Commission officials stated that they intended to conduct certain security risk management activities near the project's projected completion. Officials further stated that FCC's life-cycle management policy was not followed on the ESN project because the commission used an iterative life-cycle methodology to accelerate deployment of the initial components of the project. They said that an accelerated approach was necessary to protect the commission's high-level executives from the security threat, as well as to meet the deployment timeline presented to congressional staff at the beginning of the project. While we agree that the security threat makes implementation urgent, using an iterative methodology would not negate the need to perform security risk management activities called for by federal guidelines and the commission's policies. FCC officials further noted that its collaboration on technical activities at weekly engineering meetings with its contractors served the same purpose as gate reviews; however, the meeting minutes do not indicate that a formal decision was made to approve requirements prior to the initial deployment.

Because FCC worked to meet previously committed project time frames rather than managing to a realistic schedule that integrated security risk management activities into the project life cycle—driven by inherent dependencies among activities and using gate reviews at major transition points—the commission limited the effectiveness of its security enhancements. Consequently, its sensitive information remained at unnecessary risk of inadvertent or deliberate misuse, improper disclosure, or destruction. In addition, increased risk exists that future ESN deployments may also contain security vulnerabilities and that costly and time-consuming rework may be necessary to correct deficiencies in the completed deployments.

FCC Has Not Consistently Implemented Key Procedures for Managing the Enhanced Secured Network Project

Given the significance of the ESN project to FCC's information security, it is important that the project be managed effectively to ensure that the project succeeds in its goal of addressing weaknesses in FCC's security controls and network architecture. Effectively managing a project entails, among other things, developing a reliable life-cycle estimate of project costs, defining and maintaining a reliable project schedule, and effectively managing project risks.

- **Cost estimation.** A reliable life-cycle cost estimate provides a structured accounting of all resources and associated cost elements required to develop, produce, deploy, and sustain a particular program, and is important to the success of government acquisition programs as it provides a basis for informed investment decision making, realistic budget formulation and program resourcing, meaningful progress measurement, proactive course correction, and accountability for results. We have reported[16] that, among other things, a reliable cost estimate is: (1) comprehensive, meaning that it accounts for all life-cycle costs associated with a program; (2) well-documented, so that it is supported by detailed documentation of the technical baseline, which provides a common definition of technical, program, and schedule parameters; (3) accurate, in that it is regularly updated so that it always reflects the current status of the program; and (4) credible, meaning that it includes appropriate contingency reserves based on an assessment of risk and uncertainty.

[16]GAO-09-3SP.

- **Project schedule.** The success of a program depends, in part, on having an integrated and reliable schedule that defines, among other things, when work activities will occur, how long they will take, and how they relate to each other. A reliable schedule provides a road map for systematic execution of a program and a means by which to gauge progress, identify and address potential problems, and promote accountability. Our research[17] has identified best practices associated with developing and maintaining a reliable schedule, including, among other things, (1) sequencing all activities, (2) integrating activities horizontally and vertically, and (3) maintaining a baseline schedule.

- **Risk management.** The discipline of risk management is important to help ensure that projects are delivered on time, within budget, and with the promised functionality. It is especially important for the ESN project, given the importance of the project to the security of FCC's computer network and information. According to best practices for acquisition,[18] the purpose of risk management is to identify potential issues that could endanger achievement of critical objectives before they occur. A continuous risk management approach effectively anticipates and mitigates risks that can have a critical impact on a project. Additionally, organizations that plan to acquire IT products and services for a project should identify and assess risks associated with the acquisition process.

FCC has not consistently implemented these project management controls in developing and deploying the ESN project. Specifically:

- **Reliable life-cycle cost estimate was not developed.** To support its request for $10 million in reprogrammed funds, FCC developed a bill of materials that identified the equipment, software, and contractor services that officials determined would be needed to develop and deploy the ESN, along with an estimate of their costs. Although project officials reported using this bill of materials as a cost estimate for the ESN project, they have not updated it to account for the project's full life-cycle costs. For example, it did not include costs for government employee efforts or costs associated with operating and maintaining the enhanced network. Officials reported that such costs were planned to be covered by FCC's existing IT operating budget.

[17]GAO-12-120G (Exposure Draft).

[18]SEI, CMMI® for Acquisition.

However, without developing a life-cycle cost estimate that is comprehensive, FCC may not have sufficient information for program and budget decisions. For example, if the costs to implement and maintain the ESN project are not fully understood or are understated, the project is at increased risk of cost overruns and resource or funding shortfalls, potentially impacting the commission's ability to implement the full range of security controls needed to secure sensitive data and systems at the commission.

- **Project schedule was not sufficiently reliable.** FCC did not establish a reliable schedule for the ESN project. The project schedule consisted of multiple schedules that were not always fully integrated. For example, one schedule was maintained by the prime contractor for the work it was contracted to perform, a second schedule was maintained by the project management support contractor to show a high-level view of all activities, and a third schedule was created by FCC to guide the deployment activities completed in July 2012. Taken together, these schedules were not sufficiently sequenced, were not horizontally or vertically traceable, and did not include a baseline. Specifically:

  - *Sequencing all activities.* As of September 2012, only 12 percent of the activities on the prime contractor's management schedule and 6 percent of the activities in the project management support contractor's schedule were logically linked to predecessor or successor activities. For example, the activity for delivering finalized requirements lacked a successor activity, implying that this activity could be delayed indefinitely without impacting other project activities. This limits FCC's ability to predict the effect on the project's end date of, among other things, delayed activities and unrealistic deadlines.

  - *Verifying that the schedule can be traced horizontally and vertically.* The separate project schedules were not integrated with one another. For example, no links existed between design activities in the prime contractor's management schedule with the high-level view contained in the project management support contractor's schedule. The lack of integration among these separate schedules reduces their usefulness for managing the project and the ability of different teams to work to the same schedule expectations.

- *Maintaining a baseline schedule.* The project did not have an established baseline schedule that showed baseline dates, forecasted dates, or actual progress to date for any activities to monitor and report project performance against targeted milestones. This reduces FCC's ability to measure progress and promote accountability.

Because of these weaknesses, it is difficult to know whether the project's planned completion date is realistic. As an integrated and reliable schedule is an essential basis for managing trade-offs between cost, schedule, and scope, the absence of such a schedule increases the risk that FCC will be faced with unexpected and difficult choices about completing the project.

- **Project risks were not fully managed.** Although FCC made efforts to document and manage certain project risks, limitations existed in the commission's management of these risks and key project risks were not taken into account. For example, although the prime contractor has begun tracking project risks, no risks had been identified before July 31, 2012, which was after deployment of the initial components of the project had begun and more than 3 months after the contractor began work. Additionally, the prime contractor did not document plans for how project risks would be addressed. Specifically, although 12 risks on the contractor's list of project risks as of August 24, 2012, had not been accepted by FCC, none of them had contingency plans documented, including 6 high-priority risks. Also, as previously discussed, we identified problems in FCC's management of the ESN project in several major areas, including information security risk management, requirements development and testing, project scheduling, and cost estimation; however, these problems were not identified by FCC as risks. Such weaknesses in managing project risk may limit the ability of the commission to identify and address cost, schedule, and performance shortfalls.

These project management weaknesses occurred, at least in part, because FCC lacked policies and guidance for project management including for cost estimation, project scheduling, and managing project risks. Additionally, commission officials stated that FCC had lacked project management expertise. According to officials, as of November 2012, the commission had established an internal project management office to address these weaknesses. Further, they stated that this office had developed a number of standard operating procedures for various project management disciplines, although additional procedures for

project management remained to be completed. Lastly, the officials stated that the office was also performing the project management functions for the ESN project, including, among other things, schedule management, cost management, and project risk management; the office also had produced a draft schedule and cost and risk documents. These are positive steps; however, until FCC updates the ESN cost estimate, finalizes a reliable schedule and fully manages project risks, it will continue to have limited ability to effectively manage and monitor the ESN project, increasing the potential that successfully mitigating the risk from cyber threats will cost more than planned and will take longer than projected.

FCC Has Established a Policy for Overseeing IT Investments, but Has Not Applied it to the Enhanced Secured Network Project

Through IT investment management, organizations define and follow a process to help senior leadership make informed decisions on competing investment options. Such investments, if managed effectively, can have a dramatic impact on an organization's performance and accountability. If mismanaged, they can result in wasteful spending and lost opportunities for improving delivery of services. Our IT Investment Management framework[19] states that an organization should establish the management structure needed to manage its investments and build the investment foundation by selecting and controlling individual projects. Once a project is selected, an organization should effectively oversee it throughout all phases of its life cycle. The organization should ensure that the project continues to meet mission needs at the expected levels of cost and risk as it develops and expenditures are incurred. If the project is not meeting expectations or if problems develop, the organization should quickly take steps to address the deficiencies.

To its credit, FCC documented its policy for selecting, controlling, and evaluating IT investments in its *Information Technology Capital Planning and Investment Control Guide*. Among other things, the policy states that ongoing IT projects are to be monitored for progress against their projected cost, schedule, performance, and expected mission benefits during their planning, acquisition, deployment, and operations. All IT projects in the commission's IT investment portfolio are to be discussed by stakeholders from across FCC on a regular basis, including project schedules and related risks or impacts that may prevent projects from meeting their target schedules. Such activities are intended to ensure that

[19] GAO-04-394G.

the commission's IT initiatives are conducted in a disciplined, well-managed, and consistent manner through timely oversight, quality control, and executive review.

However, FCC did not consistently conduct regular oversight of the ESN project in accordance with its investment policy. Although FCC held monthly project management review meetings where many of the commission's IT projects were discussed by stakeholders, the ESN project was not discussed at these meetings because, according to FCC officials, only those projects under FCC's Programming Services contract—which does not include the ESN project—were included in the project management reviews.

Two oversight activities that were being performed for the ESN project include (1) periodic reviews by the CIO of a summary report of performance information on all IT projects and (2) quarterly briefings to congressional staff. However, the summary report and quarterly briefings contained limited cost, schedule, and performance data on the project. To illustrate, the quarterly congressional briefings on the status of the project were not based on measurable performance data and did not include key project activities. For example, although the August 2012 briefing slides described schedule progress as "on track," the slides did not indicate that several activities, including requirements development, were significantly behind schedule.

Officials stated that they did not update or expand the schedule section of the quarterly briefing because of the concern that doing so would increase the complexity of their presentation beyond an acceptable level. Nevertheless, without providing such information, FCC may limit the ability of congressional staff and others with oversight responsibilities to provide meaningful oversight, thus increasing the risk that the project may not meet its objectives.

Conclusions

In response to a security breach, FCC has undertaken a variety of activities to enhance the security of its network. However, because FCC deployed the initial components of the project without performing key security risk management and life-cycle management activities called for within its own policies—such as completing security and functional requirements, conducting risk management framework steps, and performing gate reviews—it limited the effectiveness of its security enhancements and did not sufficiently protect the initial deployments from the security threats that the project is intended to mitigate. In addition, the

commission's ability to successfully achieve the objectives of the project has been hindered by weaknesses related to ESN project management and oversight activities. Although the commission reported that the project is within cost and on schedule, the lack of a reliable life cycle cost estimate and project schedule, inconsistent management of project risks, and inconsistent oversight may leave FCC management and Congress without sufficient awareness of the total life-cycle costs for developing and deploying the ESN, sufficient assurance that the commission will be able to successfully complete the project by its scheduled completion date, and adequate understanding of potential obstacles to the success of the project. These shortcomings existed, at least in part, because of a lack of FCC guidance on project management, including cost estimating, scheduling, and risk management. Unless FCC more effectively implements its IT security policies, improves its project management practices, and conducts regular oversight in accordance with commission policies, unnecessary risk exists that the ESN project may not succeed in its purpose of effectively protecting the commission's systems and information.

Recommendations for Executive Action

To help strengthen IT and project management controls over the ESN project, we recommend that the Chairman of the FCC take the following seven actions:

- Perform key security risk management activities for the ESN project including selecting and documenting the security controls, assessing the implementation of the controls, and authorizing the system to operate.
- Conduct appropriate gate reviews, such as the Requirements Approval, at major transition points in the project.
- Develop a life-cycle cost estimate for the ESN project that reflects current project status.
- Establish an integrated and reliable master schedule for the ESN project.
- Document, evaluate, and manage all identified project risks in a risk management process, and document mitigation strategies for all risks.

- Commit to a time frame for establishing commission guidance on project management, including cost estimating, scheduling, and risk management.
- Monitor and oversee the ESN project on a regular basis and ensure that project data used for this purpose are current and valid.

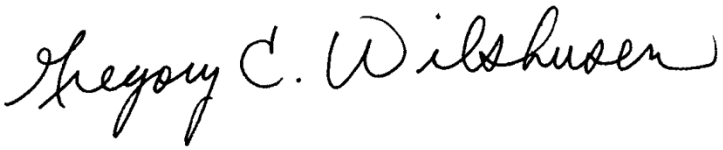
In a separate report with limited distribution, we are also making 26 recommendations associated with 21 findings to resolve technical information security weaknesses related to access controls and configuration management of the ESN.

Agency Comments

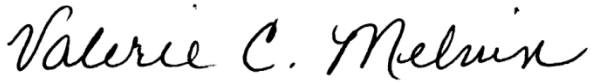
In providing written comments (reprinted in app. II) on a draft of this report, the Managing Director of FCC stated that the commission largely concurred with our findings and recognized the need to maintain an effective and forward-leaning cybersecurity program, and noted that it had multiple ongoing cybersecurity initiatives dedicated to this purpose, including the ESN project. He further noted that the commission had taken steps to strengthen its IT management resources, such as forming a new project management office. The Managing Director's comments were also accompanied by an attachment containing FCC's responses to our seven recommendations. Within this attachment, the commission concurred with all of the recommendations and described ongoing and planned actions to address them.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 7 days from the report date. At that time, we will send copies of this report to interested congressional committees and to the Chairman of the Federal Communications Commission. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

Should you or your staffs have questions on matters discussed in this report, please contact Gregory C. Wilshusen at (202) 512-6244, Valerie C. Melvin at (202) 512-6304, or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov, melvinv@gao.gov, and barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues



Valerie C. Melvin
Director, Information Management and Technology Resources Issues

Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering

Appendix I: Objectives, Scope, and Methodology

Our objectives were to assess the extent to which the Federal Communications Commission (FCC) has (1) effectively implemented appropriate information security controls for the initial components of its Enhanced Secured Network (ESN) project; and (2) implemented appropriate procedures to manage and oversee its ESN project.

To determine whether FCC has effectively implemented appropriate information security controls for the initial components of its ESN project, we reviewed equipment, software, and security tools that had been deployed at the time of our review at FCC's facility in Washington, D.C. Using National Institute of Standards and Technology (NIST) standards and guidance and FCC's policies, procedures, practices, and standards, we evaluated controls by

- reviewing the complexity and expiration of password settings to determine if password management was enforced;
- observing methods for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- assessing configuration settings to evaluate settings used to audit security-relevant events and discussing and observing monitoring efforts with FCC officials;
- inspecting key network devices and workstations to determine whether critical patches had been installed or were up-to-date; and
- examining the configurations of network- and host-based security tools to determine the extent to which they protected servers and workstations.

In addition, we assessed whether FCC had established and implemented a disciplined life-cycle management approach integrated with information security on ESN by comparing FCC's policies for system life-cycle management and cybersecurity to NIST guidance on security risk management and to widely accepted practices for system acquisition. We also compared documentation of ESN project activities and plans to these requirements and practices, and interviewed commission officials about FCC's policies and ESN's information security practices.

To determine the extent to which FCC has implemented appropriate procedures to manage and oversee its ESN project, we evaluated FCC's capabilities to employ the following key controls: cost estimating,

scheduling, project risk management, and IT investment management. The scope and methodology for our assessment of each of these is discussed below:

- *Cost estimating.* To determine the extent to which FCC reliably estimated the costs for the ESN project, we compared the practices used in deriving the project's cost estimate to best practices documented in the GAO Cost Estimating and Assessment Guide,[1] which states that a reliable cost estimate is comprehensive, well-documented, accurate, and credible. As part of this, we reviewed the estimate and supporting documentation, and interviewed commission officials about the estimate and reasons for the deficiencies we identified.

- *Scheduling.* To determine the extent to which FCC developed and maintained a reliable schedule, we analyzed the project schedule as of September 2012 against the 10 best practices documented in the Exposure Draft of the GAO Schedule Assessment Guide.[2] These include, for example, capturing all activities, integrating activities horizontally and vertically, and maintaining a baseline schedule. We also interviewed project officials about the schedule, the practices used in developing it, and reasons for deficiencies we identified.

- *Project risk management.* To assess whether FCC effectively managed the risks associated with executing the ESN project, we compared FCC's risk management practices to best practices for system acquisition.[3] In doing so, we reviewed the risk management plan, risk logs, and related documentation of project plans and activities. We also interviewed commission officials about these processes and the risks facing the project, as well as reasons for deficiencies we identified.

- *IT investment management.* To assess whether FCC made effective decisions about selecting the project and is providing sufficient oversight, we compared FCC's investment management practices to

[1]GAO-09-3SP.

[2]GAO-12-120G (Exposure Draft)

[3]SEI, CMMI® for Acquisition.

statutory requirements in the Clinger Cohen Act[4] as well as relevant sources of best practices for IT investment management.[5] In doing this, we reviewed FCC's policy for IT investment management and reviewed documentation such as agency e-mail discussions about the decision to invest in ESN, reports on project activities, and briefings to congressional staff. We also interviewed commission officials about the selection and oversight of the ESN project.

We conducted this performance audit from May 2012 to January 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[4]40 U.S.C. §§11311–11313.

[5]GAO-04-394G.

Appendix II: Comments from the Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

January 4, 2013

Mr. Gregory C. Wilshusen
Director, Information Security Issues,
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Wilshusen,

Thank you for the opportunity to review and comment on the U.S. Government Accountability Office's (GAO) draft report entitled, "Information Security: Federal Communications Commission Needs to Strengthen Controls Over Enhanced Secured Network Project."

The Commission has taken a number of steps throughout the past year to strengthen its information security, including implementing enhanced perimeter controls, malware protection and monitoring devices, and upgrading workstations to operating systems with improved security. Today, the FCC's network is stronger, better, and more secure than it was before the Commission started these upgrade efforts. The Enhanced Secured Network (ESN) Project, which GAO analyzed for this report, is only one part of these overall systems security initiatives.

We very much appreciate the support that the Commission has received from Congress to undertake these important investments, as well as the work that GAO has done to support Congressional oversight of this project. We look forward to demonstrating the effectiveness of these security initiatives, including the ESN project, after their completion in 2013, and to showing how the Commission has addressed the risks identified in its own analysis and highlighted in the GAO report.

As the report notes, the FCC, while upgrading its systems security monitoring capabilities in August 2011, engaged outside experts to assist with analysis and software tool support. Through this process, the FCC discovered an information security incident resulting from a cyber-based attack. In light of this urgent situation, the FCC quickly developed an emergency response plan — eventually termed the ESN project — that ran in parallel to its ongoing security initiatives. This plan was unlike a standard technology deployment process. It was designed to avoid any increased security risks posed by delays in implementation while keeping the FCC fully operational and maintaining the public's and industry's ability to interact with the Commission.

Throughout this project, the FCC's program management strategy was to be agile in its response to the situation so that it could bolster the security of its network as quickly as possible. The FCC monitored its risks and held regular management meetings to ensure that the project stayed on time, on budget, and on plan for the deliverables, and to ensure that risks were effectively managed. As a result, the ESN project will be completed under budget and with only minor schedule deviations. In addition the effectiveness of the FCC's network security has continually improved throughout the project. The GAO's review of this project covers a period of time during which the Commission faced an unusual level of urgency, and we look forward to sharing our further progress with Congress and GAO at a later time, when these security initiatives are more fully deployed and developed.

The FCC's overall network security is in a better place now as a result of the ESN project. Furthermore, the Commission has also taken steps to strengthen information technology management resources at the Commission, including efforts to form a new Project Management Office. Nevertheless, the Commission's staff is well-aware of the fact that the job of protecting its systems is never truly done and will require continued vigilance. The FCC's long-term strategy has been, and will continue to be, to maintain an effective and forward-leaning cyber security program that protects the agency from the growing incidences of sophisticated cyber-based threats to Federal information systems.

We thank GAO for their time and effort in working with the FCC on this important topic and appreciate the opportunity to review and comment on the draft report. Attached are the FCC's responses to the specific recommendations made in your report. The Commission largely concurs with GAO's findings and is either currently implementing them, or is planning to do so in the near future. Thank you for giving us the opportunity to outline the FCC's comprehensive on-going security enhancement efforts. We look forward to continuing to work with GAO in the future.

Sincerely,

David Robbins
Managing Director

Enclosure

Page 2

Federal Communications Commission
Comments to the Draft GAO Report Entitled
"Information Security: Federal Communications Commission Needs to Strengthen Controls Over Enhanced Secured Network Project"
(GAO-13-155, January 2013)

Recommendation 1: Perform key security risk management activities for the ESN project including selecting and documenting the security controls, assessing the implementation of the controls, and authorizing the system to operate.

Management Response: Concur. As noted in the audit report, "FCC's life cycle management policy integrates information security risk management activities into its life cycle management processes…" Because of the perceived risk to FCC systems and data resulting from the incident in September 2011, the FCC conducted abbreviated security risk management activities to accelerate the deployment of the Enhanced Secured Network (ESN) project. With regards to assessing the implementation of the controls, the FCC agrees that risk management activities for ESN should be completely and formally documented. The Program Management Office (PMO), which was recently established by the FCC to manage its broader information technology portfolio, is currently performing risk management with the ESN Schedule. Furthermore, the FCC's Chief Information Security Officer (CISO) and the CISO's supporting team have established security control programs to remediate potential risks in the process by which the FCC selects and documents its security controls and assesses their implementation. Finally, the CISO's team is working to strengthen the FCC's processes for authorizing systems to operate.

Recommendation 2: Conduct appropriate gate reviews, such as the Requirements Approval, at major transition points in the project.

Management Response: Concur. The FCC agrees that it is important that the project have appropriate reviews of key decisions in order to mitigate project risks. The FCC is currently performing reviews utilizing the ESN project management team to identify risks, handle them, and ensure the project continues to move forward at the same time. The FCC agrees that documentation and artifacts from these reviews should be maintained as evidence of this process being used during the project life cycle. Finally, the FCC is also working to update its Systems Development Life Cycle (SDLC) guidance to account for situations that require the expediency that was necessary here.

Recommendation 3: Develop a life-cycle cost estimate for the ESN project that reflects current project status.

Management Response: Concur. FCC has developed an integrated project schedule as discussed in response to Recommendation 4 below and has "loaded resources" to that schedule to form the basis for a life-cycle cost estimate for ESN. Because ESN is an on-going incident response and some of the risk mitigation pre-dated the start of the ESN project, the FCC is expanding the scope of the integrated project schedule to include all costs for the incident response going back to September 2011. Project costs are now and will continue to be managed and tracked using an Earned Value Management (EVM) system. Utilizing the EVM systems allows the project team to track costs at the task level to allow for comparison to forecasted costs for deliverables and to facilitate detailed review and analysis of costs for all work tasks.

Recommendation 4: Establish an integrated and reliable master schedule for the ESN project.

Management Response: Concur. The FCC has completed this task, has the schedule under baseline control, and project risk monitoring is done daily against the integrated schedule to ensure the reliability and integrity of the project schedule.

Recommendation 5: Document, evaluate, and manage all identified project risks in a risk management process, and document mitigation strategies for all risks.

Management Response: Concur. Throughout the project, the FCC monitored the risks associated with the project and held regular management meetings to ensure that the project stayed on time, on budget, and on plan for the deliverables, and to ensure that risks were effectively managed. As noted in the response to Recommendation 1, the FCC agrees that these meetings need to be documented more formally than in the past. With the recent establishment of FCC's PMO for information technology projects, the FCC is now maintaining a risk register in its enterprise-level project management tool where risks are linked to specific tasks in the integrated project management schedule discussed above under Recommendation 4. Each agreed-upon risk either has a risk mitigation strategy identified or under development document in the tool. All project risks are managed and tracked for mitigation for the ESN project on a daily basis by the PMO using project portfolio management software.

Recommendation 6: Commit to a timeframe for establishing commission guidance on project management, including cost estimating, scheduling, and risk management.

Management Response: Concur. As noted in the audit report, the FCC has strong policies for SDLC, Cyber Security, and its Information Technology Capital Investment Planning and Control Guide. The FCC has supplemented these policies with Standard Operating Procedures (SOPs) from the newly-created PMO; these SOPs are now being implemented. Among other topics, the SOPs address project management, and related costing estimated, scheduling and risk management.

Recommendation 7: Monitor and oversee the ESN project on a regular basis and ensure that project data used for this purpose is current and valid.

Management Response: Concur. The FCC held regular management and technical review meetings throughout the project to ensure that the project stayed on time, on budget, and on plan for the deliverables, and to ensure that risks were effectively managed. Through the FCC's recently established PMO, the FCC has stepped up monitoring and oversight of ESN and the PMO has been monitoring the ESN project on a daily basis.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov
Valerie C. Melvin, (202) 512-6304, melvinv@gao.gov
Dr. Nabajyoti Barkakati, (202) 512-4499, barkakatin@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Gary Austin, Nick Marinos, and Christopher Warweg, Assistant Directors; Sher'rie Bacon; William Cook; Saar Dagani; Rebecca Eyler; Krzysztof Pasternak; Matthew Snyder; and Michael Stevens made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.