U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Accessible Version

October 07, 2020

Congressional Requesters

National Security: Additional Actions Needed to Ensure Effectiveness of 5G Strategy

The federal government and private industry are preparing for the next generation of wireless technology, which has the potential to represent the most significant change in wireless networks since cellular service was introduced. This fifth generation of mobile communication networks, or 5G, may have transformative effects that will increase productivity, contribute to the growth of new businesses, and spur innovation in sectors beyond telecommunications, including transportation, manufacturing, medicine, and others. Specifically, 5G will offer increased bandwidth, constant connectivity, and faster network response times, which can enhance and expand mobile technologies for consumers and businesses and introduce tens of billions of new devices to harness the Internet.[1] However, while the advent of 5G could create significant economic opportunities, it also introduces national security risks as malicious actors seek to exploit these new 5G technologies.

Several federal organizations have roles in and responsibilities for addressing national security risks associated with 5G and enabling its deployment.

- **National Security Council (NSC).** NSC is the President's principal forum on national security and foreign policy matters—including 5G—and coordinates among various government agencies.[2] NSC also assesses and evaluates national security risks to the United States and its global security interests, including risks posed by 5G, in order to make recommendations to the President.
- **National Economic Council (NEC).** NEC advises the President on U.S. and global economic policy and monitors the implementation of the President's economic policies, including those related to 5G.[3]
- **White House Office of Science and Technology Policy (OSTP).** OSTP provides the President with analysis and advice on technology-related aspects of national security, including 5G, and leads science and technology policy coordination across the federal government. The office also provides analyses on the application and use cases of 5G technologies and their potential impact on the federal government.

[1]Wireless carriers in the United States are currently deploying "hybrid" 5G, which uses 5G technologies in combination with existing 4G networks to improve the networks' speed. In the future, carriers may deploy "standalone" 5G, which relies exclusively on 5G equipment to allow for additional enhanced capabilities.

[2]NSC is comprised of the President, the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Energy, and other officials as designated by the President. See 50 U.S.C. § 3021(c)(1). Additionally, the Assistant to the President for National Security Affairs is responsible for determining the agenda for the NSC, at the direction of the President.

[3]NEC is chaired by the President and is comprised of the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Agriculture, the National Security Advisor, the Assistant to the President for Economic Policy, the heads of other executive departments and agencies, and other officials as designated by the President. See Exec. Order No. 12835, 58 Fed. Reg. 6189 (Jan. 27, 1993).

- **Department of Commerce's National Telecommunications and Information Administration (NTIA).** NTIA provides advice to the President on telecommunications, including 5G, and manages programs that deal with expanding the use of spectrum and internet access.[4] NTIA also addresses and manages risks related to the 5G supply chain, spectrum management, and technology development.

You asked us to evaluate the federal government's efforts to mitigate challenges and national security risks related to 5G. We have previously reported on the challenges of deploying 5G and 5G technology and associated challenges for the federal government.[5] Additionally, we have an ongoing classified review that identifies and evaluates national security risks associated with 5G technologies and efforts taken to address those risks. This report examines the extent to which the Administration has developed a national strategy on 5G that address our six desirable characteristics of an effective national strategy.[6]

To conduct this work, we reviewed recent policy and strategy documents, relevant statutes, and documents issued by the current administration, such as the *National Cyber Strategy*, Executive Order 13873 on *Securing the Information and Communications Technology and Services Supply Chain*, and the Secure 5G and Beyond Act of 2020.[7] We also reviewed the *National Strategy to Secure 5G of the United States of America* (5G national strategy) to determine the extent to which it addresses the characteristics of an effective national strategy.[8] To do this, we reviewed the content of the 5G national strategy to determine the extent to which it addresses the elements in each of our six desirable characteristics.[9] Specifically, two analysts conducted separate assessments of the 5G national strategy using a three-point scale to rate the inclusion of each element of the desirable characteristic in the strategy. The strategy "fully addresses" a characteristic when it includes all elements of that characteristic; "partially addresses" a characteristic when it includes some, but not all elements of the characteristic; and "does not address" a characteristic when it does not include any elements of the characteristic. The two analysts met to determine whether their individual assessments of the extent to which each characteristic of the 5G national strategy addresses the elements of the desirable characteristics were in agreement with each other. Finally, a third analyst reviewed the

[4]Spectrum refers to the radio frequencies used to communicate over the airwaves. NTIA and the Federal Communications Commission jointly manage spectrum within the United States; NTIA manages the federal use of spectrum, and the Federal Communications Commission manages non-federal use of spectrum.

[5]GAO, *5G Deployment: FCC Needs Comprehensive Strategic Planning to Guide Its Efforts,* GAO-20-468 (Washington, D.C.: June 12, 2020) and *5G Science and Tech Spotlight: 5G Wireless,* GAO-20-412SP (Washington, D.C.: Mar. 27, 2020).

[6]In our prior work, we identified six desirable characteristics of an effective national strategy by consulting numerous sources, including statutory requirements and legislative and executive branch guidance. These six characteristics are each subdivided into various elements. GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

[7]White House, *National Cyber Strategy* (Washington, D.C.: September 2018); Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019); and, Secure 5G and Beyond Act of 2020, Pub. L. No. 116-129 (Mar. 23, 2020).

[8]White House, *National Strategy to Secure 5G of the United States of America* (Washington, D.C.: March 2020).

[9]As we testified in GAO 04-408T, our six desirable characteristics are (1) defining purpose, scope, and methodology; (2) outlining problem definition and risk assessments; (3) identifying goals and objectives, and outcome-related performance measures; (4) a description of resource, investments, and risk management; (5) a clear delineation of organization roles, responsibilities, and mechanisms for coordination; and (6) a description of how the strategy is integrated and implemented.

assessments, and all three analysts reached a final consensus on the assessments of each desirable characteristic.

We also interviewed relevant officials at OSTP and NTIA on their efforts to draft, develop, or implement the 5G national strategy and its implementation plan. Additionally, we requested to meet with NSC officials and provided questions as part of this engagement. However, NSC declined to meet with us, provide answers to our questions, or provide comments on a draft copy of this report.

We conducted this performance audit from May 2020 to October 2020 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.

Background

The *National Cyber Strategy*, issued in September 2018, describes actions that federal agencies and the administration are to take to secure critical infrastructure, among other things.[10] For example, one of the strategy's goals is to foster a vibrant and resilient digital economy. To achieve this goal, the strategy outlines a number of priority actions, such as investing in next-generation infrastructure. The strategy states that the administration will facilitate the accelerated development and rollout of next-generation telecommunications and information communications infrastructure and will work with the private sector to facilitate the evolution and security of 5G. Additionally, the *National Cyber Strategy Implementation Plan* designated the Executive Office of the President and NSC, along with coordination from other federal agencies, as the lead entity to finalize and implement a 5G cybersecurity strategy.

In response to concerns about 5G's potential effect on national security, Congress passed the Secure 5G and Beyond Act of 2020*,* Pub. L. No. 116-129 (Mar. 23, 2020). Among other things, it requires the President, in consultation with relevant federal agencies, to develop a strategy to secure and protect 5G systems and infrastructure in the United States and provide technical assistance on 5G security to mutual defense treaty allies, strategic partners, and other countries. In March 2020, the White House issued the 5G national strategy to provide direction on how the U.S. government will secure 5G infrastructure domestically and abroad. According to OSTP officials, NSC led the interagency coordination process to draft the strategy and coordinated through the cyber policy coordination committee, which included various federal organizations such as the Department of Defense, the Department of State, the Department of Commerce and NTIA, and the Federal Communications Commission.[11] Additionally, the 5G national strategy states that NEC is primarily coordinating the private sector-led domestic rollout of 5G.

The Secure 5G and Beyond Act of 2020 also requires the President, within 180 days of the enactment of the act, to develop and submit an implementation plan that provides a description of U.S. national and economic security interests related to 5G, an assessment of potential

[10]*National Cyber Strategy.*

[11]According to *National Security Presidential Memorandum 4*, policy coordination committees are typically used to manage the development and implementation of national security policies with multiple executive departments and agencies. *See* 82 Fed. Reg. 16881 (April 4, 2017).

security threats and vulnerabilities to 5G infrastructure, and options to identify and mitigate 5G risks, among other things.[12] Additionally, in May 2020, NTIA, on behalf of the administration, requested public comments to inform the development of the implementation plan and to accelerate the development and deployment of 5G infrastructure in the United States. In June 2020, NTIA received 80 public comments from domestic and foreign private companies and associations, private citizens, non-profit organizations, and local governments. According to NTIA officials, they are in the process of analyzing these comments in order to inform the NTIA officials, they are in the process of analyzing these comments in order to inform the implementation plan and contribute to a more accelerated rollout of 5G.

The 5G Strategy Partially Addresses Some, but Not All, of Our Desirable Characteristics of a National Strategy

The March 2020 5G national strategy partially addresses five of our desirable characteristics of an effective national strategy and does not address one, as summarized in table 1. We have previously identified a set of six desirable characteristics that, when included in a national strategy, would provide additional guidance to responsible parties for developing and implementing national strategies.[13] These six characteristics are subdivided into various elements that, when included, make it easier for the responsible parties to implement the strategy and achieve its goals. For example, elements for the purpose, scope, and methodology characteristic include information on the strategy's purpose, how the strategy compares and contrasts with other national strategies, activities it covers, theories that guided its development, impetus for the strategy, and definitions of key terms. We continue to believe that it is a best practice for national strategies to include all elements of our six desirable characteristics to guide federal agencies and other parties responsible for achieving results, evaluating progress, and ensuring accountability.

Table 1: Extent to Which the March 2020 *National Strategy to Secure 5G* (5G National Strategy) Addresses Our Desirable Characteristics of a National Strategy

Desirable characteristic	Elements of the desirable characteristic that should be addressed in a national strategy	Our assessment of the 5G national strategy against the elements of the desirable characteristics
Purpose, scope, and methodology	Why the strategy was produced, the scope of its coverage, and the process by which it was developed	Partially addresses
Problem definition and risk assessment	What the particular national problems are, assessments of the risks to critical assets and operations—including the threats to, and vulnerabilities of, critical operations—and discussion of the quality of data available regarding the risk assessment	Partially addresses
Goals, subordinate objectives, activities, and performance measures	What the strategy is trying to achieve; steps to achieve those results; and the priorities, milestones, and performance measures that include measurable targets to gauge results and help ensure accountability	Partially addresses
Results, investments, and risk management	What the strategy will cost and the types of resources and investments needed	Does not address

[12]The Secure 5G and Beyond Act of 2020 required the implementation plan to be developed and submitted to the appropriate committees of Congress by September 23, 2020.

[13]GAO-04-408T.

Desirable characteristic	Elements of the desirable characteristic that should be addressed in a national strategy	Our assessment of the 5G national strategy against the elements of the desirable characteristics
Organizational roles, responsibilities, and coordination	Who will implement the strategy, what their roles will be, and mechanisms to coordinate their efforts	Partially addresses
Integration and implementation	How a national strategy relates to other strategies' goals, objectives, and activities and to subordinate levels of government and their plans to implement the strategy	Partially addresses

Source: GAO analysis of the 5G strategy | GAO-21-155R

Note: In line with the methodology described in GAO-04-408T, we consider a national strategy to fully address a characteristic if it explicitly includes all elements of that characteristic. We consider it to partially address a characteristic if it includes some, but not all elements of the characteristic, and we consider it to not address a characteristic if it includes none of these elements. GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

Purpose, scope, and methodology.

The 5G national strategy *partially addresses* the purpose, scope, and methodology characteristic.[14] For example, in the introductory letter to the strategy, the President identifies its purpose and writes that the strategy is intended to lead the development, deployment, and management of secure and reliable 5G communications infrastructure worldwide and that it will explain how to ensure the security, reliability, and trustworthiness of 5G infrastructure. The strategy also includes information about its scope and mission areas by identifying its four lines of effort as (1) facilitating domestic 5G rollout; (2) assessing the risks and identifying core security principles for 5G infrastructure; (3) managing the risks to economic and national security from the use of 5G infrastructure; and (4) promoting responsible global development and deployment of 5G infrastructure.

However, the strategy does not define key terms or include information on how it was developed. Specifically, the strategy does not address its methodology, including which principles or theories were used to guide its development, what organizations or offices drafted the document, or which parties were consulted in its development. NTIA officials told us that the strategy was developed as part of an interagency coordination process through NSC's cyber policy coordination committee, but the text of the strategy does not include this level of information. A national strategy without a complete description of its purpose, scope, and methodology is less useful to the entities it is intended to guide and to oversight organizations such as Congress.

[14]Examples of elements that should be included in the purpose, scope, and methodology characteristic: statement on the strategy's purpose; how the strategy compares and contrasts with other national strategies; major functions, mission areas, or activities it covers; principles or theories that guided its development; impetus for the strategy (e.g. statutory requirement or event); process to produce the strategy; and a definition of key terms.

Problem definition and risk assessment.

The 5G national strategy *partially addresses* the characteristic of defining the problem and performing a risk assessment.[15] Specifically, the strategy discusses the problem that it is intended to address and broadly identifies underlying vulnerabilities, threats, and risks. For example, the strategy states that malicious actors seek to exploit 5G technology and that 5G infrastructure is a target-rich environment for adversaries because it includes a large amount of data and devices. Further, the strategy states that adversaries will seek to steal information for monetary gain and may also disrupt public and private services that rely on communication infrastructure. NTIA officials told us that the administration used best practices such as the Prague Proposals, identified at the Prague 5G Security Conference, to inform the strategy's information on 5G risks and the strategy states that it will synchronize its security principles with the best practices identified in the Prague Proposals.[16]

However, the strategy does not include a risk assessment or complete information on 5G risks and does not include information on the quality (constraints or deficiencies) of the data. The strategy narrowly focuses on cybersecurity and supply chain risks to 5G infrastructure and does not include the full breadth of 5G risks.[17] However, it is unclear whether these risks were identified as the result of a risk assessment. National strategies that do not have an analysis of threats and vulnerabilities as part of a broader risk assessment cannot adequately inform management decisions about resource allocations required to minimize risks and maximize returns on resources expended.

Goals, subordinate objectives, activities, and performance measures.

The 5G national strategy *partially addresses* the goals, subordinate objectives, activities, and performance measures characteristic.[18] Specifically, the strategy establishes a hierarchy of goals and subordinate objectives and includes some activities to address some 5G risks. As we previously mentioned, the strategy identifies its purpose and objective and corresponding lines of efforts for 5G risks related to cybersecurity and the supply chain. The strategy also provides information on some activities within each line of effort that are needed to achieve its goals. For example, within the line of effort to promote responsible global development and deployment of 5G, the strategy discusses the objective of promoting U.S. leadership of international standards

[15]Examples of elements that should be included in the problem definition and risk assessment characteristic: discussion or definition of problems, their causes, and operating environment; risk assessment, including an analysis of threats and vulnerabilities; and quality of data available, (e.g., constraints, deficiencies, and "unknowns").

[16]In May 2019, the Czech Republic hosted the Prague 5G Security Conference, which included officials from over 30 countries and resulted in a set of recommendations for nations to consider as they design, construct, and administer their 5G infrastructure.

[17]In our ongoing classified review on 5G national security risks, we identify categories of national security risks associated with 5G technologies that were developed using responses from the Department of Defense, the Department of State, the Central Intelligence Agency, and the Office of the Director of National Intelligence. The 5G national strategy does not cover all of the categories that we identified.

[18]Examples of elements that should be included in the goals, subordinate objectives, activities, and performance measures characteristic: overall results desired, (i.e., "end-state"), hierarchy of strategic goals and subordinate objectives; specific activities to achieve results; priorities, milestones, and outcome-related performance measures; specific performance measures; process for monitoring and reporting on progress; and limitations on progress indicators.

development and includes specific actions, such as expanding federal interagency coordination in standard-setting organizations.

However, the strategy does not identify or discuss the importance of establishing priorities, milestones, performance measures with measurable targets, or a process for monitoring and reporting on progress. If the strategy does not identify clear desired results and priorities, specific milestones, and outcome-related performance measures, entities may not understand what they should try to achieve or what steps are required to achieve the desired results.

Results, investments, and risk management.

The 5G national strategy *does not address* the characteristic of results, investments, and risk management.[19] Specifically, the strategy does not explicitly discuss what it will cost and does not include any cost estimates either for achieving individual goals or for implementing the strategy as a whole. Additionally, the strategy does not include information on the sources and types of resources required, such as federal, state, local, or private resources. This is of particular concern because 5G deployment will occur across all levels of the government and the private sector, and addressing 5G risks and challenges will be a shared fiscal responsibility. Without a strategy that provides guidance on resource, investment and risk management, implementing entities will not be able to allocate resources and investments according to priorities and constraints, track costs and performance, and shift such investments and resources as appropriate.

Organizational roles, responsibilities, and coordination.

The 5G strategy *partially addresses* the characteristic of describing organizational roles, responsibilities, and coordination mechanisms.[20] Specifically, the strategy identifies some roles and expectations of the federal agencies and departments that will be implementing the strategy. For example, the strategy states that NEC, in coordination with other organizations, will facilitate the private sector-led domestic rollout of 5G.

However, most often the strategy assigns its goals and activities broadly to the administration or the U.S. government and does not delegate the responsibility to specific federal agencies or departments. The strategy also does not establish or provide information on an accountability and oversight framework or identify a process for coordination or conflict resolution. Without this information, organizations and other stakeholders will not be able to foster coordination and clarify specific roles, particularly where there is overlap, and thus will not be able to enhance both implementation and accountability.

[19]Examples of elements that should be included in the results, investments, and risk management characteristic: resources and investments associated with the strategy; types of resources required, such as budgetary, human capital, information technology, research and development, contracts; sources of resources, (e.g., federal, state, local, and private); economic principles, such as balancing benefits and costs; resource allocation mechanisms, such as grants, in-kind services, loans, or user fees; “tools of government,” (e.g., mandates or incentives to spur action); importance of fiscal discipline; linkage to other resource documents (e.g., federal budget; and risk management principles).

[20]Examples of elements that should be included in the organizational roles, responsibilities, and coordination characteristic: roles and responsibilities of specific federal agencies, departments, or offices; roles and responsibilities of state, local, private, and international sectors; lead, support, and partner roles and responsibilities; accountability and oversight framework; potential changes to current organizational structure; specific processes for coordination and collaboration; and how conflicts will be resolved.

Integration and implementation.

The 5G national strategy *partially addresses* the integration and implementation characteristic.[21] Specifically, the strategy discusses how it is integrated with other national strategies and plans. For example, the strategy states that it is intended to fulfill the goals of the *National Cyber Strategy* and expand on how the U.S. government will secure 5G infrastructure. It also provides text from the *National Cyber Strategy* that is applicable to 5G, thereby highlighting common and shared goals and demonstrating its relationship with the *National Cyber Strategy*. The 5G national strategy also refers to additional strategies, such as NTIA's *National Spectrum Strategy* and the Federal Communications Commission's strategy to *Facilitate America's Superiority in 5G Technology Plan,* and it provides details on their efforts as part of the overall effort to facilitate domestic 5G rollout.[22]

However, the 5G national strategy does not contain information regarding planned subordinate strategies, although federal agencies have issued subordinate strategies since the issuance of the 5G national strategy. For example, in May 2020, the Department of Defense issued its 5G strategy, which is the department's approach to implementing the 5G national strategy, and in August 2020, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency released its 5G strategy, which establishes its five strategic initiatives.[23] Both of these strategies are in line with the overarching 5G national strategy.

The 5G national strategy also does not contain information regarding an implementation plan. The *Secure 5G and Beyond Act of 2020* required the President to develop and submit an implementation plan to the 5G national strategy by September 23, 2020. According to NTIA officials, NSC and NEC started developing this implementation plan in the spring of 2019. Additionally, according to OSTP officials, the implementation plan should provide guidance and define roles for the implementing organizations when it is finalized. According to these officials, the implementation plan will assign activities and roles based on the lines of effort within the strategy. Further, OSTP expects to be assigned to activities related to "5G and beyond" research and development and the international testing environment. National strategies that do not include information that clarifies the relationships between various implementing entities, both vertically and horizontally, run the risk of not being able to foster effective implementation and accountability.

Uncertain if Implementation Plan Will Include All Elements of Our Desirable Characteristics

According to NTIA and OSTP officials, the 5G national strategy was intentionally written to be at a high level and as a result, it may not include all elements of our six desirable characteristics of national strategies. These officials stated that the 5G implementation plan required by the

[21]Examples of elements that should be included in the integration and implementation characteristic: integration with other national strategies (horizontal); integration with relevant documents from implementing organizations (vertical); details on specific federal, state, local, or private strategies and plans; implementation guidance; and details on subordinate strategies and plans for implementation (e.g., human capital) and enterprise architecture.

[22]Earlier this year, we found that the *Facilitate American's Superiority in 5G Technology Plan* did not clearly identify specific and measurable performance goals or measures. Without such strategic planning efforts, the Federal Communications Commission will be unable to determine the effectiveness of its efforts. GAO-20-468.

[23]Department of Defense, *Department of Defense (DoD) 5G Strategy* (Washington, D.C.: May 2, 2020). Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *5G Strategy: Ensuring the Security and Resilience of 5G Infrastructure In Our Nation* (Washington, D.C.: Aug. 19 2020).

Secure 5G and Beyond Act of 2020 is expected to include specific details, not covered in the 5G national strategy, on the U.S. government's response to 5G risks and challenges. The implementation plan is expected to align and correspond to the lines of effort in the 5G national strategy. NTIA officials told us that the implementation plan to the 5G national strategy would be finalized by the end of October 2020.[24] However, the officials we spoke to were unable to provide details on the final content of the implementation plan such as whether the plan would include all elements of our six desirable characteristics of national strategies given that it was not final. National strategies and their implementation plans should include all elements of the six desirable characteristics to enhance their usefulness as guidance and to ensure accountability and coordinate investments. Until the administration ensures that the implementation plan includes all elements of the six desirable characteristics, the guidance the plan provides decision makers in allocating resources to address 5G risks and challenges will likely be limited.

Conclusions

National strategies and their implementation plans can be used to help manage emerging issues that affect national security, such as 5G. Our six desirable characteristics, when included in a national strategy, can help shape policies and programs to achieve intended results. Further, national strategies are not final, but rather starting points.[25] As such, there is room for the implementation plan to include elements from our desirable characteristics that will enable federal agencies and departments to effectively develop policies and make resource allocations that will enable the successful oversight, deployment, and use of 5G technologies in partnership with private industry. 5G is currently being developed and deployed within the United States—and across the world—and is considered vital to U.S. interests. As a result, it is vital for the U.S. government to have a 5G strategy and implementation plan that contain enough information and details to effectively position the nation to be able to plan for and respond to the advent of 5G.

Recommendation

The Assistant to the President for National Security Affairs, in coordination with relevant stakeholders from NSC and NEC, should ensure that the plan to implement the 5G national strategy fully addresses all elements of our six desirable characteristics of a national strategy.

Agency Comments

We provided a copy of this draft report to NSC, NEC, OSTP, and NTIA for review and comment. NTIA provided technical comments, which we incorporated as appropriate. OSTP and NSC stated that they had no comments and NEC did not provide a response to our draft report.

- - - - -

We are sending copies of this report to the appropriate congressional committees, the Assistant to the President for National Security Affairs, the Director of NEC, the Director of OSTP, the

[24]As stated above, the Secure 5G and Beyond Act of 2020, was enacted on March 23, 2020 and required the President to develop and submit the 5G implementation plan by September 23, 2020. We requested to meet with NSC officials. However, NSC declined to meet with us, provide answers to our questions, or provide comments on a draft copy of this report.

[25]GAO, *National Capital Region: 2010 Strategic Plan is Generally Consistent with Characteristics of Effective Strategies*, GAO-12-276T (Washington, D.C.: Dec. 7, 2011).

Secretary of Commerce, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Brian Mazanec at (202) 512-5130 or mazanecb@gao.gov or Nick Marinos at (202) 512-9342 or marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Kaelin Kuhn (Assistant Director),

Kush Malhotra (Assistant Director), Erika Prochaska (Assistant Director), Jamilah Moon (Analyst-In-Charge), Tracy Barnes, Anastasia Kouloganes, Joanne Landesman, and Andrew Stavisky.

Brian M. Mazanec
Director, Defense Capabilities and Management

Nick Marinos
Director, Information Technology and Cybersecurity

List of Requesters

The Honorable James M. Inhofe
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Marco Rubio
Acting Chairman
The Honorable Mark R. Warner
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Eddie Bernice Johnson
Chairwoman
Committee on Science, Space, and Technology
House of Representatives

The Honorable Adam B. Schiff
Chairman
The Honorable Devin Nunes
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

The Honorable Bill Foster
Chairman
Subcommittee on Investigations and Oversight
Committee on Science, Space, and Technology
House of Representatives

The Honorable Richard Burr
United States Senate

The Honorable Mikie Sherrill
House of Representatives

(104323)