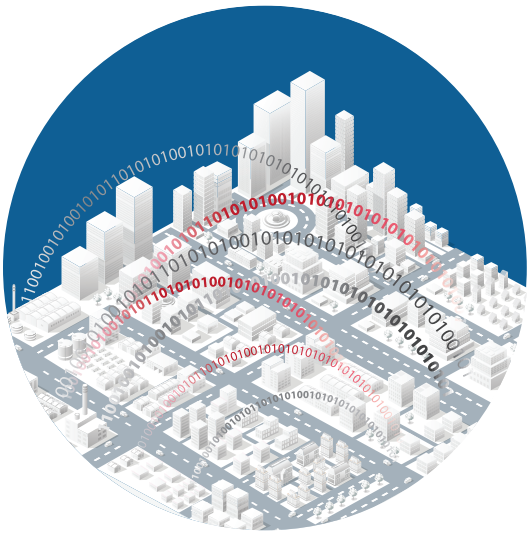
Thinking Forward About Federal Civilian Cybersecurity 2016

MITRE

Approved for Public Release; Distribution Unlimited. 16-2991 (c)2016 The MITRE Corporation. ALL RIGHTS RESERVED



Bringing Federal Mission Execution and Cybersecurity Closer Together

Our nation and the world are in the midst of a digital transformation.[1] Technologically, this digital transformation seemingly connects anything to anything. Socially, this increasingly networked world changes how people live and work, and how organizations deliver goods and services. This transformation enhances the ability of federal civilian government organizations[2] to execute their many missions by improving how they use networked technology[3] and data to deliver information and services to the public.[4]

This tighter connection between networked technology and mission execution also means that cyber attacks and disruptions pose risks to the ability of federal civilian government organizations to execute their missions. Every day, federal civilian networks and systems are under cyber surveillance, reconnaissance, and attacks from adversaries. Every day, these networks and systems are vulnerable to disruption from natural events such as storms. Successful attacks and disruptions can result in "mission breaches" that damage public trust, and national and economic security, as they can place information confidentiality, availability, and integrity, as well as human safety and infrastructure reliability, at risk.[5] Therefore, cybersecurity is not just about securing technology and data; it is about helping organizations manage risk so they can operate and sustain mission-essential services to the public through cyber attacks and disruptions.

As mission execution is increasingly intertwined with networked technology, enterprise mission strategy and enterprise cybersecurity strategy must be inextricably linked. Organizations across the world are starting to change the paradigm that relegates cybersecurity to a handful of executives and teams to address and are making the security of their systems and data a top business issue for the organization as a whole.[6] Similarly, government leaders with responsibility for mission operations, policy, planning, and management must join forces with Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) to chart paths forward that enable organizations to realize the promise, and address the perils, of network technology for mission execution.[7]

We wrote this paper for federal civilian government leaders who play roles across their enterprises and who have the opportunity to collaboratively set the direction for their organization's mission and cybersecurity strategies in the coming years. In keeping with the premise of a risk-based approach, we don't offer a single one-size-fits-all prescription. We do present a range of technical and non-technical ideas to help you develop and execute strategies to integrate mission and cyber priorities. In total, we believe these ideas can help manage risk, move the scales in your favor, raise the cost to adversaries, and limit the harm from disasters.

We set the stage with two pieces of context to inform your strategic choices.

- **Cyber Ecosystems:** From both cyber governance and operational perspectives, individual organizations work across a range of government and non-government organizations and individuals to execute their missions. The related technical and mission to interdependencies should inform next steps.
- **Policy and Programmatic Building Blocks:** Over the past years, different administrations and Congresses have passed laws and enacted government-wide policies and programs to improve federal cyber risk management. Together, these provide a number of blocks that organizations can build on as they move forward.

We then explore four broad areas, and a set of related concepts, that can help bring together your mission and cyber priorities.

- **Adaptive Defense:** Cyber defenders face a dynamic environment where they must be able to anticipate and quickly adapt to threats in order to support ongoing mission performance. Organizations can become more adaptive by: using approaches to counter advanced adversaries both before they enter networks and after they have breached networks, collaborating across ecosystems and using shared information to tailor defenses, and adopting resilience approaches that increase the likelihood of

continued mission execution in the face of attack or disruption.

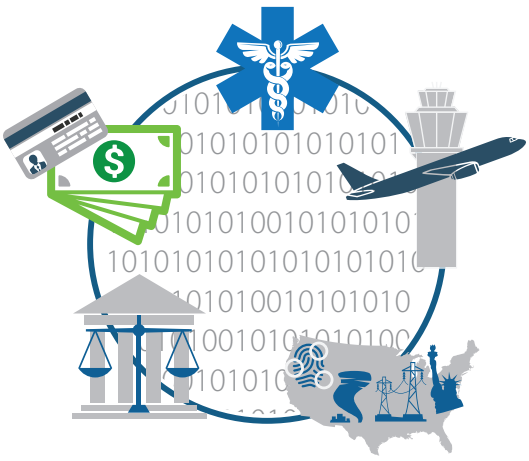
- **Holistic Risk:** Cybersecurity has often focused on risks to data confidentiality, availability, and integrity—such as theft of intellectual property. Changing technologies (e.g., Internet of Things, Cyber–Physical Systems) used in support of mission performance require cyber defenders to take a more holistic view of risk and also consider physical risks to human safety and infrastructure reliability. Organizations can strengthen their ability to address holistic risk by determining what level of assurance is needed to address the holistic risk in the converged technologies they will use and preparing for incidents that have both information and physical consequences.
- **Trusted Technologies and Users:** As increasing numbers of networked devices play increasingly important roles in mission execution, the need for stronger trust in both the systems and the humans who use them increases. Organizations can increase the trustworthiness of their technologies by bringing greater focus to security engineering at each stage of the system life cycle and tailoring the level of trust needed by a system or user based on how a system will be used.
- **Shared Mind-set:** More than any technical issue, human mind–sets and attitudes are critical to address the challenges that lie at the intersection of mission execution and cybersecurity. Organizations can enhance this shared mind–set by communicating the relationship between mission performance and cybersecurity, making clear that cybersecurity is not just a static compliance exercise but requires ongoing evolution and continuous improvement, and building organizational structures that enable cross–organizational and cross–ecosystem collaboration.

We conclude by exploring how you can use different leadership levers of authority and influence—**direction setting, team and talent building, coalition building,** and **decision making**—to move forward with these ideas and concepts.

As different federal civilian government branches, departments, and agencies have different missions with different levels of cybersecurity risk, and are at different stages in addressing the intersection of mission execution and cybersecurity, we intentionally present ideas at a relatively high level so that individual organizations can tailor and learn more about them, as appropriate.

Moreover, in recent years, much has been written and discussed about cybersecurity. Therefore, we synthesize a range of ideas and concepts which, depending on your background, may be more or less familiar. For a busy reader, we hope to provide a relatively quick and summative way to help frame and prioritize future choices.

The intersection of government mission execution and cybersecurity is a particular focus of The MITRE Corporation, which operates federally funded research and development centers (FFRDCs). MITRE works at the intersection of technology, planning, and mission operations and has several decades of experience working across federal branches, departments, and agencies to strengthen mission performance and cybersecurity.



Context: Think Ecosystems Not Islands

When considering the interplay between mission execution and cybersecurity, individual government organizations are part of cyber ecosystems, not cyber islands. The term "ecosystem" describes a set of interconnected participants that interact in changing ways for multiple purposes. Ecosystems are not defined in legislation, nor do they appear on organizational charts. They are a useful, conceptual way to demonstrate that federal branches, departments, and agencies do not govern and use networked technologies in isolation.[8]

From a governance perspective, heads of federal civilian branches, departments, and agencies are responsible for executing their missions and maintaining their organization's cybersecurity commensurate with their risk.[9] This means that there is understandable and even necessary variability among organizations in how they address cybersecurity. At the same time, there are other organizations with cybersecurity policy and programmatic responsibilities that impact all executive branch departments and agencies.[10] These organizations, and their federal civilian cybersecurity responsibilities, include:

- **The Office of Management and Budget (OMB):** OMB oversees the implementation of agency-specific and government-wide cybersecurity programs.
- **The Department of Homeland Security (DHS):** DHS provides operational leadership for federal civilian cybersecurity, executes several government-wide cybersecurity programs, and plays roles in incident response and investigation.
- **The National Institute of Standards and Technology (NIST):** NIST issues and updates security standards for information systems used by federal agencies.
- **The Department of Justice (DoJ):** DOJ investigates many cyber threats and incidents including those affecting federal organizations.
- **The General Services Administration (GSA):** GSA supports cross-government acquisition of cybersecurity applications and services.

Federal civilian government organizations also work across and outside the federal government to execute their core missions in ways that use information technology and manage cyber risk. For any given organization, the specific ecosystem members will differ based on the mission area (e.g., financial, aviation, homeland security, health care, judiciary, agriculture). Ecosystems can include a mix of federal, state, and local government agencies, private companies and not-for-profit organizations, and individuals who interact for many purposes.

Specific ecosystem members play roles including providing policy and regulatory guidance; electronically managing, sharing, and using information to enhance service delivery; developing, deploying, integrating, operating, and maintaining networked technologies and services; providing security services and capabilities; and using services. In total this leads to numerous interdependencies and electronic pathways within and across ecosystem members. As networked technologies are increasingly likely to have an impact in the physical world (e.g., "smart buildings," self-driving cars, medical devices) ecosystem risks include safety and infrastructure reliability that go beyond traditional cybersecurity concerns of confidentiality, availability, and integrity.

While each ecosystem will be different, each organization should understand its cyber ecosystem and consider what a healthy and effective ecosystem would look like and how it should operate. For example: How do ecosystem members effectively and securely collaborate? How do ecosystem members and systems demonstrate trust? These types of questions will inform subsequent sections of this paper.

Context: Government–Wide Policy and Programmatic Building Blocks

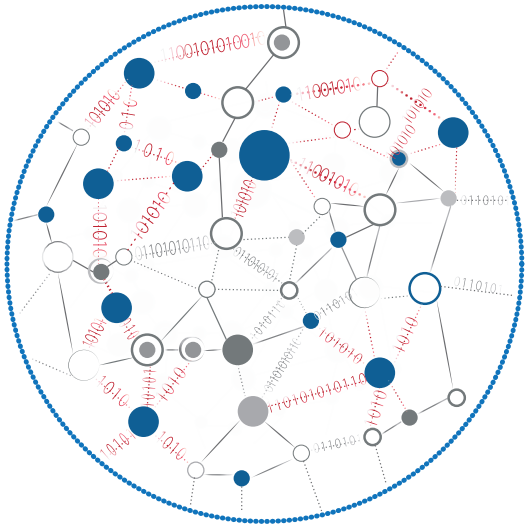
As federal leaders contemplate next steps to strengthen the integration between mission execution and cybersecurity, there are several existing policies and programs that provide important building blocks. In addition to work individual organizations are already doing, different administrations and Congresses have passed laws and enacted government–wide policies and programs to improve cyber risk management.[11] Recent actions include the 2015 Cybersecurity and Implementation Plan (CSIP) for the Federal Civilian Government and the 2016 Cybersecurity National Action Plan (CNAP) which together establish both near–term and longer term actions to strengthen cybersecurity.[12] Below is an overview of some of the building blocks that have been put in place over the past several years.

- **Risk Management:** Cyber threats are a risk to be continually managed, not a problem to be solved once for all time. This risk management approach has influenced federal law, policy directives, and guidance that require agencies to maintain security programs appropriate to the level of risk they face. It has also influenced development and deployment of government–wide continuous diagnostic and mitigation tools to identify cybersecurity risks within systems.[13]
- **Policy and Guidance:** A broad range of policy and guidance informs implementation of federal cybersecurity programs, the development of system controls, and the execution of mitigation activities.[14] This policy and guidance addresses a range of areas, including but not limited to vulnerability patching, identifying and prioritizing high–value assets, data breach notifications, and multifactor authentication. Recently, the Administration created a federal CISO position to develop, manage, and coordinate cybersecurity policy, planning, and implementation across executive agencies and issued a policy directive to clarify federal responsibilities for responding to significant cyber incidents.[15]
- **Threat Information Sharing:** The federal government has placed a priority in law, policy, and operations on threat information sharing across public and private sector organizations. This priority recognizes that threats to an organization today can threaten other organizations tomorrow and that sharing information can strengthen an organization's ability to adapt its defenses.[16]
- **Boundary Protection and Monitoring:** The federal government has sought to make it more difficult for adversaries to breach federal networks and for threats to spread by strengthening government–wide perimeter protection. This has included securing classified networks, reducing and consolidating external network connections, and developing and deploying government–wide intrusion detection, protection, and analysis capabilities.[17]
- **Cybersecurity as Cross-Government Service:** There have been several efforts to offer cross–government cybersecurity services so that individual agencies are not left alone to defend against cyber threats. These efforts include provision of intrusion detection, protection, and analysis capabilities and continuous diagnostic and monitoring services as described above. More recently, OMB and GSA are taking steps to expand government–wide shared services for cybersecurity.[18]
- **Cyber Workforce:** Several government–wide efforts have sought to close the gap between the cybersecurity workforce that is needed and the cyber workforce that is available. Efforts have included use of special hiring authorities, expansion of training, and increasing the number of cyber defense teams.[19]
- **Evolving Technology Environment:** As the technology landscape rapidly changes, there have been a variety of approaches to help the federal government adapt to this changing environment.

They include development of reference architecture for mobile technology security; a standardized approach to the assessment, authorization, and continuous monitoring of cloud computing services; the development of a Federal Cybersecurity Research and Development Strategic Plan; and the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which addresses control-systems-related security incidents and mitigations. The federal government has also determined that some legacy technology systems are so difficult to secure that they should be retired and replaced with new systems.[20]

- **Critical Infrastructure Collaboration:** Our nation's national and economic security, as well as the ability of individual organizations to execute their mission, is dependent on a broad range of critical infrastructure sectors (e.g., energy, financial services, transportation, communications) that are primarily owned and operated by the private sector. The federal government has developed several policies, plans, and approaches that promote voluntary public-private collaboration with these critical sectors to share cyber information and manage cyber risk.[21]
- **Strengthening Connections between Civilian and National Security Agencies:** Some cyber threats to federal civilian systems come from foreign nation-states or threat actors. It is important, therefore, for civilian agencies to effectively coordinate with national security agencies. To this end, the federal government has developed coordination mechanisms, such as federal cyber operations centers, to manage the sharing of appropriate information.[22]

While the work is not completed, these policies and programs demonstrate that the federal government has taken many steps to strengthen and improve cybersecurity. Together, they provide a number of blocks that organizations can build upon as they identify their next steps to address the continually evolving technology and threat environments.



Adaptive Cyber Defense

The Adaptive Cyber Defense Challenge: Cyber defenders seek to deter adversaries by making it more difficult to execute successful attacks and easier to limit the damage from attacks. In practice, deterrence is challenging, in part, because of the dynamic nature of the threat.

A variety of human actors (e.g., nation-states, criminals and criminal organizations, terrorists and terrorist organizations) and natural events (e.g., severe weather) threaten federal ecosystems. Human actors, especially the most capable (i.e., advanced persistent threats), evolve their approaches and capabilities to evade detection and establish footholds in systems. Signature-based defenses, which compare network traffic to known malicious patterns, can work at the scale and speed needed but can only address known threats. Malware detection doesn't help identify adversaries who use mechanisms that don't require malware, such as credential theft, to "live off the land" of the systems they attack.[23]

At the same time, the number of networked technologies continually increases. The amount of data that crosses these networks, and missions that data supports, rises. Thus, the attack surface that must be defended expands. Taken in total, leaders face an environment where cyber defenders must be able to anticipate and quickly adapt to threats in order to support ongoing mission performance.

Thinking Forward about Adaptive Cyber Defense: As federal approaches to cyber defense evolve over the coming years, leaders should think forward about how their organizations can continually adapt to evolving threats. These efforts can evolve from existing building blocks such as boundary protection and monitoring, threat information sharing, and efforts to strengthen resilience. Below are some specific areas for consideration:

Beyond Perimeters and Signatures: Perimeter-and signature-based approaches that block known threats from entering a network are an important component of comprehensive cyber defense. However, they are not sufficient. Advanced adversaries breach perimeter defenses. In a diverse ecosystem of multiple technologies and organizations, it is difficult to define perimeters in the first place, and adversaries don't always use or need malware to breach systems.[24] Leaders should be thinking about how their organizations:

- Identify adversaries through their cyber behaviors in addition to their cyber signatures
- Use threat-based approaches to identify, understand, disrupt, counter, and deceive adversaries throughout the attack life cycle (e.g., reconnaissance, weaponize, deliver, exploit, control, execute, and maintain), both before they enter networks and after they have breached networks.[25]

Sharing to Using: Sharing information is an important way to strengthen cyber ecosystems. For example, sharing threat information across an ecosystem can help all members better understand adversary behaviors. However, information sharing is a means to an end—adapting defenses based on anticipated new attacks—not an end itself. As organizations increasingly share information, the questions will increasingly shift from "should we share," or "how do we share," to "how do we use." Leaders should be thinking about how their organizations:

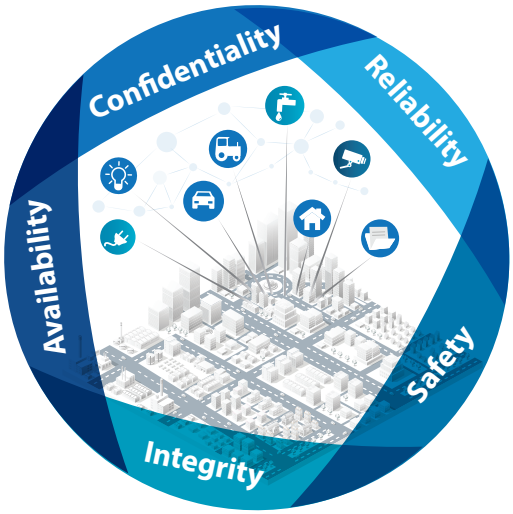
- Analyze and contextualize shared information to make it usable (e.g., relevant and actionable)
- Use shared information to tailor cyber defenses
- Identify which elements of analysis and adaptation can be automated and which require skilled human intervention
- Promote policies, systems, and processes that foster cross-ecosystem collaboration to address common threats and risks.

Mission Resilience: Cyberattacks and disruptions will happen. The mission must still be performed. Therefore, mission-essential functions must be able to continue under duress. Put more simply, organizations must be able to operate resiliently.[26] Cyber attacks and disruptions may challenge existing assumptions about the ability to maintain business continuity. Leaders should be thinking about how their organizations:

- Identify, tailor, and implement appropriate resilience techniques (e.g., redundancy, diversity, unpredictability) that enable systems and processes to perform mission-essential functions through a cyber attack or disruption
- Restore full mission functions subsequent to a successful cyber attack or disruption.

Adaptive Defense Outcomes: As leaders think forward about adaptive defense, what sort of outcome statements would you like to make about your organization? Here are a few outcomes for your consideration:

- The impact of attacks and disruptions is minimized.
- Our organization maintains mission-essential functions in the face of attack or disruption.
- Our organization rapidly restores full mission function subsequent to a successful attack or disruption.
- Our organization rapidly adjusts our defenses to changing risks.
- The public trusts our organization to safeguard its data and execute our cyber-enabled mission safely and securely.



Holistic Risk in a CyberPhysicalHuman World

The Holistic Risk Challenge: Cybersecurity risk management has often focused on understanding and addressing risks to data confidentiality, availability, and integrity—such as theft of intellectual property or personal identity information.[27] Changing technologies require that we expand the scope of risk. Now, physical risks to human safety and infrastructure reliability must become part of the cybersecurity equation.

This change is occurring because information systems, which inform human decisions, are increasingly converging with operational, or control, systems that have an impact on the physical world. There are many commonly used terms to describe these converged technologies, including Internet of Things, Cyber-Physical Systems, Industrial Control Systems, and the Industrial Internet. This paper calls them CyberPhysicalHuman because they both inform human decision making and have impact in the physical world.[28]

Whatever term you use, federal ecosystems will increasingly include many converged technologies and systems. These converged technologies offer potentially appealing features, such as cost savings, energy efficiency, and productivity gains, that could enhance the ability of organizations to improve mission performance and service to the public. Examples include greater energy efficiency from "smart buildings," improved healthcare from embedded medical devices, and safer and more efficient transportation from self-driving cars.

The challenge for organizations will be to balance these potential mission benefits with potential mission risks. The number of converged technologies will expand the number of potential targets for adversaries. They also add risks—for example, patient and passenger safety—that have not traditionally been a major concern for many information technologies, and should not be thought about "after the fact." These trade-offs will inform the technologies organizations use and the types of incidents that may require response. Organizations may encounter incidents that have information security, physical safety, and infrastructure reliability consequences.

Thinking Forward about Holistic Risk: Over the coming years, leaders should be thinking forward about how their organizations understand, prioritize, and address the holistic risk associated with the converged technologies they may use. A focus on holistic risk builds off the overarching federal risk management building block: the level of cybersecurity should be appropriate to the level of risk faced. Additionally, it builds off, and can inform next steps the government takes to address, the emerging technology environment. Below are some specific areas for consideration:

Understand Holistic Risk in the Context of Mission and Function: When considering how to use converged technologies to improve mission performance, organizations will need to consider a broad set of trade-off questions, as safety and reliability take their place next to confidentiality, availability, and integrity. There is no single formula for this balancing act. Instead, the level of safety and security should be based on how an organization actually intends to use a technology and its data to support mission functions. Leaders should be thinking about how their organizations:

- Intend to incorporate converged technologies and their associated data to execute their mission functions
- Identify risks to both information loss and physical harm to people and infrastructure, based on how converged technologies and their data will actually be used to execute mission functions
- Establish the level of assurance (i.e., the confidence that a technology will perform as expected), based on intended functional use, that is needed in converged technology design, development, integration, operations, and maintenance

- Determine which individuals in an organization can make what level of decisions to use and incorporate converged technologies
- Develop holistic security architectures that address both information security and physical safety and understand the threats to, and interdependencies between, converged systems.

Humans in the Holistic Risk Equation: As the distinctions between cyber and physical risks blur, distinctions between the different types of security roles that humans play and the type of incidents they will respond to will also blur. Leaders should be thinking about how their organizations:

- Prevent, protect against, respond to, and recover from incidents that impact physical safety, infrastructure reliability, and information security[29]
- Promote integration and collaboration between physical security and information security teams
- Enable humans to secure technologies in a way that is seamless and transparent
- Identify where human "overrides" for technologies that can have a physical impact are needed or possible.

Policy Evolution: As new technologies continue to blur the boundaries between cyber and physical, between human and machines, it will be important to examine related policy guidance. This means that leaders should be thinking about how their organizations:

- Provide adequate policy guidance to address the holistic risks that emerge from this evolving technology landscape and identify what steps are needed to fill potential gaps.

Holistic Risk Management Outcomes: As leaders think forward about holistic risk, what sort of outcome statements would you like to make about your organization? Here are a few outcomes for your consideration:

- Our organization understands and addresses the holistic safety and security risks associated with the different technologies that we use to enhance mission execution.
- Our organization effectively responds to incidents that impact both information security and physical safety in a coordinated and integrated manner.

Trusted Technologies and Users

The Trust Challenge: Our world's digital transformation depends on trust. People and organizations trust systems to securely share data with other systems, safeguard data, and provide information and services to users. People and organizations trust that users of systems are who they say they are. Yet, time and again networked technologies have proven to be vulnerable to various forms of malicious activity, which can leave them deemed untrustworthy.

As with many ideas in the world of cybersecurity, the need to strengthen confidence in the trustworthiness of the underlying systems and the users of those systems is not new. The need for more secure design can be traced to foundational cybersecurity work in the early 1970s.[30] The need for system controls (e.g., authentication, access control) to address system and human risks has been a focus in policy and guidance. However, as increased numbers of networked technologies play increasingly important roles in mission execution, the need for stronger trust in both the systems that are used and the humans who use them increases.

Thinking Forward about Trust: As federal uses of technologies evolve to improve mission performance, leaders should be thinking forward about how their organizations increase the underlying trustworthiness in the technologies and the people who use them. These efforts can build off existing building blocks of standards, guidelines, and strategies, such as a recent NIST publication about systems security engineering.[31] Below are some specific areas for consideration:

Holistic Trust: Regardless of whether a government organization acquires technology from diverse supply chains or designs its own technology, there are opportunities to influence the security of a technology throughout its life cycle—design, development, integration, operations, maintenance, and disposal. For example, identifying how suppliers use security engineering in system design; promoting quality software design; collaborating across the government to encourage manufacturers to provide solutions that effectively integrate mission and security requirements; identifying which resilience techniques should be used in systems; and determining how systems will be integrated, configured, and managed in a secure manner. Leaders should be thinking about how their organizations:

- Securely engineer technologies and software across the system life cycle
- Promote acquisition approaches that safely and securely integrate technologies into mission execution.

A Continuum of Trust: Trust shouldn't be an all-or-nothing proposition. There are several important approaches which, in combination, allow organizations to establish different trust thresholds for different users and systems. For example, authentication helps establish that users are who they say they are. Access controls help establish that users are authorized to take certain actions. Network segmentation helps separate systems and users on the basis of their mission criticality and trustworthiness. Assurance helps establish the confidence that systems and controls will perform as intended based on some level of evidence. This diversity of methods, combined with assurance, provides an opportunity for organizations to think about trust as a continuum: for example, determining what systems and data are mission essential, what level of assurance is needed for which systems, and what level of authentication should be required for users to access which systems and data. Leaders should be thinking about how their organizations:

- Determine which systems and data require higher or lower levels of trust for humans or systems to access them
- Tailor security methods based on the level of trust needed to access a system or data
- Assure that third-party providers can provide the appropriate level of trust based on the systems and data with which they interact.

Trust Outcomes: As leaders think forward about trust, what sort of outcome statements would you like to make about your organization? Here are a few outcomes for your consideration:

- Our organization acquires, deploys, and operates technology that can safely and securely support mission execution.
- Our organization understands what levels of trust are required for humans or systems to access different systems and data and tailors our security methods appropriately.

Shared Mindset

The Mindset Challenge: What mind-set do individuals and organizations bring to cybersecurity? Is cybersecurity viewed primarily as a technology challenge that is divorced from "the real mission work"? Is cybersecurity viewed primarily as a "check the box" compliance exercise? To what extent is risk management about technical analysis or a way of thinking about the organization's mission? These are mind-set questions that go beyond any particular policy or technology. They are also vital pieces of the cybersecurity equation that haven't been fully solved.

If our nation could manage cybersecurity risk by writing a policy, developing a plan, or recognizing the need for secure systems, our work would be done. Many of the fundamental challenges and conceptual solutions in cybersecurity are not new. For example, the previous section discussed trust challenges. This is not a new issue. In 1970, the Defense Science Board published a seminal report about security controls for computer systems. It noted, for example, that "it is important to influence designers of future computers and software so that security controls can be installed before the fact and as an integral part of the system."[32] Yet, 46 years later, the 2016 Federal Cybersecurity Research Development Plan notes that "today virtually every computing system is vulnerable to some form of malicious cyber activity. While continuous improvements in systems security are being made, progress is often ad-hoc and difficult to measure."[33]

There are many reasons for disconnects between problem identification and solution development. Cost and speed to market/deployment considerations can override security in trade-off decisions. Cyber defenders must protect an increasingly large space, where an adversary only needs to find one vulnerability to exploit. When considering the digital transformation, another factor emerges. This transformation exists at the intersection of people and technology. Therefore, human mind-set, as much as technical specifications, is an essential part of the cybersecurity tool kit. It is vital to make cybersecurity accessible, understandable, and "part of how we do things around here" for everyone.

Thinking Forward about Mind-set: As federal approaches to addressing the enduring cybersecurity challenges evolve, leaders should be thinking forward about how their organizations can change mind-sets about cybersecurity and its relationship to mission execution. These approaches can evolve from existing education, communication, cyber workforce, and cybersecurity cross-government service building blocks. Below are some specific areas for consideration:

Making Risk and Resilience Real: Risk management and resilience concepts are both vital to manage cybersecurity in today's threat environment. Execution of these concepts can involve technical analysis and solutions. However, in the absence of a clear connection to mission and mission impact, they can quickly become abstract. In contrast, a clear understanding of the relationship between mission, risk, and resilience can support the identification and appropriate tailoring of security and resilience controls. Moreover, it can make what can be abstract concepts real to people who are responsible for mission execution and can help those mission owners play a more effective role in the discussion of security tailoring and tradeoffs. Leaders should be thinking about how their organizations:

- Translate risk and resilience concepts in ways that meaningfully and understandably connect mission execution to cybersecurity for individuals across the organization
- Bring together personnel with mission, technology, and security backgrounds to collaboratively identify mission risk and resilience issues and develop tailored solutions.

Striking the Balance between Continuous Improvement and Compliance: A desire for compliance with policy and guidance is understandable, and some level of compliance is an important component of a strong cyber defense. However, in the dynamic world of cybersecurity where adaptation to changing threats is

vital, a primarily compliance-based approach can become a static "paperwork and checklist" exercise, which can stand in the way of necessary continuous improvement. For example, certain compliance requirements may become outdated. Or, better ways may emerge or exist to address the underlying challenge. Equally important, if individuals perceive that cyber security compliance is the primary goal, then it can create a misperception that the challenge ends when compliance is met. Finally, as different organizations manage different levels of mission risk, one-size-fits-all compliance regimens are not needed. It is important, therefore, to strike the balance between compliance and continuous improvement so that they can complement each other and evolve together. Leaders should be thinking about how their organizations:

- Promote adaption of policies and processes that enable and reward continuous improvement, learning, and agile adaptation to address changing cyber threats
- Encourage individuals and teams to make positive cases for tailored security controls based on mission risks rather than defend why they may not be using a specific control
- Evolve compliance approaches to recognize changes in the technology and mission landscapes.

Playing a Team Sport: While every federal organization is responsible for its own cybersecurity, effectively managing cyber risk requires a team, rather than an individual, mind-set. This team mind-set can inform collaboration at different levels to understand and address a range of issues. These can include the relationship between mission execution and cybersecurity; cross-ecosystem cyber threats; and identification and development of a workforce and external providers that can effectively integrate cybersecurity into mission execution. Leaders should be thinking about how their organizations:

- Promote governance, management and operational structures that enable cross-organizational and cross-ecosystem engagement and collaboration to address cybersecurity
- Attract and obtain employees and service providers who can effectively integrate cybersecurity into mission execution.

Shared Mind-set Outcomes: As leaders think forward about shared mind-set, what sort of outcome statements would you like to make about your organization? Here are a few outcomes for your consideration:

- Our organization understands the relationship between our mission execution, our technology, and our risk.
- Our organization enables and rewards people and teams who adapt cybersecurity to changing risks to our mission.
- We work effectively across our organization and ecosystem to address cybersecurity challenges to mission execution.
- Our organization attracts and obtains the employees and service providers needed to effectively integrate cybersecurity into our mission execution.

Leadership Levers

This paper offers federal civilian government leaders a range of ideas that can be used to build off recent federal actions, and focus and frame strategic direction and priorities over the coming years. These ideas intentionally link mission execution with cybersecurity. We hope this connection, more than any specific action, will guide organizations moving forward. This connection brings together the different people and perspectives in an organization toward a common purpose and in a single conversation: how to reduce cyber risk in order to realize our mission on behalf of the American people.

Where can you go next? Organizations will continue to grapple with discrete security and technology issues that pose mission risks in the coming years. In keeping with the premise of a risk-based approach, there isn't a single, one-size-fits-all prescription. Organizations should continually assess their current cybersecurity posture, identify gaps, analyze alternatives, and tailor their security controls appropriately. Frameworks such as NIST's "Risk Management Framework" and "Framework for Improving Critical Infrastructure Cybersecurity" are useful tools to assist in this process.[34]

However, technical challenges associated with the important work of identifying and tailoring security controls are not the most critical challenge facing government leaders. It is the challenge of altering mind-sets, attitudes, and perspectives. It is here—where people, not systems, are most important—that leadership is most vital. From the users of government systems who may click without thinking, to managers whose teams may not have all the tools needed to get the job done, to senior executives who must balance what they want to do but may feel hampered by checklist mentalities and compliance reward systems, setting the right leadership tone for an organization may be the difference between page 1 of the Washington Post and the Presidential Rank Award.

With this in mind, we conclude by exploring how leaders might use different levers of authority and influence in their "leadership toolkit." To provide a common perspective, we look to the core qualifications for the federal government's Senior Executive Service to identify and derive some levers that leaders can draw on:[35]

- **Direction Setting** (i.e., leading change)
- **Team and Talent Building** (i.e., leading people and business acumen)
- **Coalition Building** (i.e., building coalitions)
- **Decision Making** (i.e., results driven and business acumen).

The following explores how each of these levers could be applied against different ideas we discuss in this paper. Determining which specific levers could be applied, and in what order, will depend on what your organization is already doing.

Direction Setting: As you set and communicate direction and guidance, consider how you link cybersecurity to mission success. You can:

- Develop a compelling narrative that demonstrates how effective cybersecurity can help your organization realize its mission and demonstrate it is worthy of the trust that the American people expect in dealing with the government.
- Communicate about cybersecurity and its relationship to mission success in ways that are understandable by all, not just cybersecurity experts.
- Recognize and embrace new strategic insights that can emerge from anywhere in the organization where individuals and teams are learning how to better address cyber threats to the organization's mission.
- Use written strategies, guidance, and personal interactions to promote specific ideas such as the importance of adaptive defense, how converged technologies will change the risks organizations face and must address, how acquisition and secure engineering can be used to strengthen technology

security, and the need to prepare for incidents that have both cyber and physical elements.

Team and Talent Building: In word and deed, consider how you clarify the need for teamwork that goes well beyond the CIO/CISO organization and identify the right talent mix to address the relationship between mission execution and cybersecurity. You can:

- Establish that governance, management, and operational structures must reflect the inherent connections between mission execution and cybersecurity and requires cross-organizational engagement between mission execution, technology, cyber security, and physical security personnel and teams.
- Convene cross-functional teams to help address specific ideas such as assessing which converged technologies may or may not be appropriate to use in furthering mission execution, developing trust continuums appropriate for the organization, or working through the normal trade-off debates that will occur in developing and executing cybersecurity strategies.
- Identity and remove barriers to individuals and teams who seek to learn and adapt agilely to changing cyber threats.
- Identify and develop individuals with skills and capabilities needed to implement ideas such as adaptive defense, identifying and addressing holistic risk, executing security engineering, making risk-informed decisions and identifying the most appropriate service delivery model (e.g., shared services, managed security services, direct hiring) to address gaps.
- Explore roles such as the Chief Risk Management Officer, which would consider risks that cut across mission and technology.

Coalition Building: As you engage outside your organization (e.g., other government agencies, commercial companies, not-for-profit organizations), you can promote policies, systems, and processes that foster cross-ecosystem collaboration to address common cybersecurity challenges to mission execution. You can:

- Convene and champion partnerships across your ecosystem to understand how organizations with similar missions and functions may be using converged technologies and determine if there are opportunities to pool resources and expertise to better understand their impacts and implications.
- Actively share effective practices and techniques with other ecosystem members.
- Build coalitions across your ecosystem that advocate on behalf of more secure and resilient approaches to technology design and development.
- Work with oversight organizations to help realize government-wide risk informed cybersecurity by promoting measures and oversight approaches that balance compliance and continuous improvement and help organizations appropriately tailor cybersecurity commensurate with the holistic risk and magnitude of harm to mission execution they face.

Decision Making: As you make cybersecurity-related investment and resource allocation decisions, consider how they will strengthen the ability of the organization to execute its mission in the face of persistent cyber attacks and disruptions. You can:

- Promote approaches in which individuals and teams are asked to make a positive case for tailored security and resilience solutions rather than defending why they may not be using a specific control.
- Place greater emphasis on approaches (e.g., identifying adversary behaviors, resilience techniques, using shared information to tailor defenses) that will strengthen the organization's ability to anticipate and adapt to cyber threats.
- Set expectations about what degree of security engineering is expected in systems whether they are acquired or developed.
- Set expectations about what level of assurance different converged technologies, or converged technologies in combination, must meet depending on how they will be used to execute mission functions.

During the coming years, we look forward to continuing to think and work forward with you and other members of our community about how we address these challenges together.

About MITRE

The MITRE Corporation is a not-for-profit organization whose sole focus is to operate federally funded research and development centers, or FFRDCs. Independent and objective, we take on some of our nation's—and the world's—most critical challenges and provide innovative, practical solutions for some of our nation's most critical challenges in defense and intelligence, aviation, civil systems, homeland security, the judiciary, healthcare, and cybersecurity. If you've ever flown in a jet or used GPS, you've benefited from technology with roots in an FFRDC. We also have an independent research program that explores new and expanded uses of technologies to solve our sponsors' problems. MITRE has principal locations in McLean, VA, and Bedford, MA, with 60 sites around the world.

Cybersecurity is a core capability within MITRE, cutting across our work for the federal government. MITRE has worked closely with government to strengthen our nation's cyber defenses for more than four decades. We work with our sponsors and industry partners to adopt effective new concepts and apply solutions in awareness, resiliency, and threat-based defense. MITRE advocates a balanced security posture that combines classic cyber defense approaches with a new emphasis on leveraging cyber threat intelligence to respond and adapt quickly to a cyber attack. To accomplish this, we encourage partnerships that promote sharing cyber threat information and effective tools. Our strategy thrives on a foundation of unrelenting innovation and operational experimentation. If you have questions, please email us at cyber@mitre.org.

1. See, for example, "Digital Life in 2025," Pew Research Center, March 11, 2014, at http://www.pewinternet.org/files/2014/03/PIP_Report_Future_of_the_Internet_Predictions_031114.pdfhttp.
2. The scope of this paper includes federal civilian branches (e.g., executive and judicial) and associated departments and agencies (D's/A's). It does not include military and intelligence agencies.
3. This paper will use the terms technology and systems interchangeably. In both cases, they will include components, applications, and networks.
4. For example, the public can go to websites such as www.usa.gov to access a range of government information and services. See also https://www.whitehouse.gov/issues/technology for a summary of different initiatives the federal government has undertaken to apply the Internet and information technology to make government more effective, transparent, and accessible.
5. For example, in 2015 more than 20 million personnel and security records held by the Office of Personnel Management (OPM) were hacked. This hack impacted OPM, the millions of people whose personal data was compromised, and the other federal D's/A's for which OPM conducted security background checks. See https://www.opm.gov/cybersecurity/cybersecurity-incidents/; and https://www.opm.gov/investigations/background-investigations/. See also "Annual Report to Congress: Federal Information Security Modernization Act," Office of Management and Budget, March 18, 2016, which identifies the number and types of reported information security incidents affecting the integrity, confidentiality, and/or availability of government information, systems, and services (https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf).
6. "Securing the C-Suite: Cybersecurity perspectives from the boardroom and C-suite," IBM Institute for Business Value, 2016.
7. This need for integration between mission and cybersecurity was recognized in the Office of Management and Budget's (OMB) 2015 Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. CSIP tasked the President's Management Council (PMC) with overseeing implementation of CSIP. The PMC comprises the Chief Operating Officers of major federal government agencies, primarily Deputy Secretaries, Deputy Administrators, and agency heads from the General Services Administration (GSA) and OPM. See "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," Office of Management and Budget, October 30, 2015, at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf; and "President's Management Council," General Services Administration, at http://www.gsa.gov/portal/content/133811
8. For a more complete discussion of cybersecurity and ecosystems, see "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action," Department of Homeland Security, March 23, 2011 at https://www.dhs.gov/enabling-distributed-security-cyberspace.
9. 44 U.S.C. § 3554, Federal Agency Responsibilities.
10. See "Annual Report to Congress: Federal Information Security Modernization Act," Office of Management and Budget, March 2016; "Addressing Threats to the Nation's Cybersecurity," Federal Bureau of Investigation, at https://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1; "Improving Government Cybersecurity," General Services Administration, at http://gsablogs.gsa.gov/technology/2016/02/01/improving-government-cybersecurity/; and "Cybersecurity," Department of Homeland Security, at https://www.dhs.gov/topic/cybersecurity. This paper focuses on cross-government roles and responsibilities; it does not seek to characterize roles and responsibilities these organizations play with non-federal organizations.
11. It is beyond the scope of this paper to identify department- and agency-specific cybersecurity policies and programs. However, as part of the federal cybersecurity governance ecosystem, individual D's and A's are affected by government-wide policies and programs.
12. See "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," op. cit.; and "Fact Sheet: Cybersecurity National Action Plan," The White House, February 9, 2016, at https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.
13. The Federal Information Security Modernization Act (FISMA) of 2002 and the FISMA Modernization Act of 2014 provide a framework for federal information security. They cover a broad range of topics and require that agencies take a risk-based approach to information security. See https://www.gpo.gov/fdsys/pkg/BILLS-107hr2458enr/pdf/BILLS-107hr2458enr.pdf and https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf. There are many examples of how this risk-informed approach has influenced policy and programs. In 2010, NIST published a risk management framework for federal information systems. See "Guide for Applying the Risk Management Framework to Federal Information Systems," National Institute of Standards and Technology, February 2010, at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf. In 2014, NIST published a voluntary cybersecurity framework to help organizations manage cybersecurity risk based on the likelihood an event will occur and its impact. See "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, February 2014, at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. In 2015, as part of its Cybersecurity Strategy and Implementation Plan, OMB required D's/A's to prioritize high-value assets that enable mission-essential functions. See "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," op. cit. The CSIP also accelerated the deployment of the DHS Continuous Diagnostics and Mitigation program, which deploys tools to agencies to provide a more accurate picture of the inventory of hardware and software assets under management and the ongoing security risks to those assets. See "Continuous Diagnostics and Mitigation (CDM)," Department of Homeland Security, at https://www.dhs.gov/cdm.
14. As part of their roles, OMB issues federal information security policies, NIST issues and develops security standards for federal D's/A's, and DHS issues Binding Operational Directives that require agencies to mitigate a particular risk to their information systems. See, for example, "Annual Report to Congress: Federal Information Security Modernization Act," Office of Management and Budget, March 18, 2016; "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," op. cit.; and "Remarks by Secretary of Homeland Security Jeh Charles Johnson on Securing the .GOV at CSIS—As Prepared for Delivery," Department of Homeland Security, July 8, 2015, at https://www.dhs.gov/news/2015/07/08/remarks-secretary-homeland-security-jeh-charles-johnson-securing-gov. A range of NIST guidance can be accessed at http://csrc.nist.gov/publications/PubsFL.html.
15. See "Fact Sheet: Cybersecurity National Action Plan," op. cit., and "Presidential Policy Directive—United States Cyber Incident Coordination," Executive Office of the President of the United States, July 26, 2016, at https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
16. There have been a number of efforts to promote information sharing. An initiative in the 2009 Comprehensive National Cybersecurity Initiative was to connect federal cyber operations centers to enhance situational awareness. See "The Comprehensive National Cybersecurity Initiative (CNCI)," Executive Office of the President of the United States, undated, at https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative. The Cybersecurity Act of 2015 established a voluntary framework for real-time information sharing of cyber threat indicators and defensive measures between the federal government and non-federal organizations. See http://docs.house.gov/billsthisweek/20151214/CPRT-114-HPRT-RU00-SAHR2029-AMNT1final. A 2015 Executive Order promoted cyber information sharing with an emphasis on cross-sector collaboration and the creation of information sharing and analysis organizations. See "Executive Order Promoting Private Sector Cybersecurity

Information Sharing," Executive Office of the President, February 13, 2015, at https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

17. See, for example, "National Cybersecurity Protection System (NCPS)," Department of Homeland Security, at https://www.dhs.gov/national-cybersecurity-protection-system-ncps; "Remarks by Secretary of Homeland Security Jeh Charles Johnson on Securing the .GOV at CSIS-As Prepared for Delivery," op. cit.; and "Information Security: DHS Needs to Enhance Capabilities, Improve Planning and Support Greater Adoption of its National Cybersecurity Protection System," Government Accountability Office, January 2016, at http://www.gao.gov/products/GAO-16-294.
18. See "Fact Sheet: Cybersecurity National Action Plan," op. cit.; and "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," op. cit.
19. See "Fact Sheet: Cybersecurity National Action Plan," op. cit.; "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," op. cit.; and "The Comprehensive National Cybersecurity Initiative (CNCI)," op. cit.
20. The need to replace legacy technology that is very difficult to secure is the premise behind a proposed Information Technology Modernization Fund in the recent Cyber National Action Plan. See "Fact Sheet: Cybersecurity National Action Plan," op. cit. Examples of other efforts to address the evolving technology environment can be found at "Annual Report to Congress: Federal Information Security Modernization Act," Office of Management and Budget, March 18, 2016; "The Comprehensive National Cybersecurity Initiative (CNCI)," op. cit.; "Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security," National Science and Technology Council, February 2016, at https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf; "Mobile Security Reference Architecture," Federal CIO Council and Department of Homeland Security, May 2013, at https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf; "FedRAMP: Program Overview," FedRAMP, undated, at https://www.fedramp.gov/about-us/about/; and "The Industrial Control Systems Cyber Emergency Response Team," Department of Homeland Security, at https://ics-cert.us-cert.gov/.
21. See, for example, "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," Department of Homeland Security, 2013, at https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf; "Presidential Policy Directive 21—Critical Infrastructure Security and Resilience," Executive Office of the President, February 2013, at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; and "Executive Order 13636—Improving Critical Infrastructure Cybersecurity," Executive Office of the President, February 2013, at https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
22. See, for example, "The Comprehensive National Cybersecurity Initiative (CNCI)," op. cit.
23. See "Living Off the Land," Secure Works, May 2015, at https://www.secureworks.com/blog/living-off-the-land.
24. The EINSTEIN platform is piloting behavioral-based analytics. See "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," op. cit.
25. Existing models can inform these threat based approaches. See, for example, "Adversarial Tactics, Techniques, and Common Knowledge," The MITRE Corporation, at https://attack.mitre.org/wiki/Main_Page; and "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, at http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.
26. "Cyber Resiliency Engineering Framework," The MITRE Corporation, January 2012, at https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework.
27. For purposes of this paper, confidentiality includes privacy considerations.
28. See, for example, "The CyberPhysicalHuman World of Homeland Security," The MITRE Corporation, at https://www.mitre.org/capabilities/cybersecurity/overview/thinking-forward/thinking-forward-archives-0; "Industrial Internet: Pushing the Boundaries of Minds and Machines," General Electric, November 2012, at http://www.ge.com/docs/chapters/Industrial_Internet.pdf; "Cyber-Physical Systems (CPS) Framework Release 1.0," Cyber Physical Systems Public Working Group, May 2016, at https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Draft_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf ; "Gartner Says 6.4 Billion Connected Things Will be in Use in 2016," Gartner, November 2015, at http://www.gartner.com/newsroom/id/3165317; and "National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the Internet of Things," National Security Telecommunications Advisory Committee, November 2014, at https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.
29. The need to respond to incidents that have both cyber and physical elements is anticipated in the recent policy directive for cyber incident coordination. See "Annex for Presidential Policy Directive—United States Cyber Incident Coordination," Executive Office of the President, July 26, 2016, at https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident.
30. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security," Rand Corporation, February 1970, at http://www.rand.org/pubs/reports/R609-1/index2.htmll.
31. See "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," National Institute of Standards and Technology, May 2016, at http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf. Other examples include "National Strategy for Trusted Identifies in Cyberspace," National Institute of Standards and Technology, at http://www.nist.gov/nstic/about-nstic.html; and "Fact Sheet: Cybersecurity National Action Plan," op. cit.
32. "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security," op. cit.
33. "Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security," op. cit.
34. See "Guide for Applying the Risk Management Framework to Federal Information Systems," op. cit., and "Framework for Improving Critical Infrastructure Cybersecurity," op cit.
35. Derived from "Senior Executive Service: Executive Core Qualifications," Office of Personnel Management, undated at https://www.opm.gov/policy-data-oversight/senior-executive-service/executive-core-qualifications/.

www.mitre.org

cyber@mitre.org

Approved for Public Release; Distribution Unlimited. 16-2991 (c)2016 The MITRE Corporation. ALL RIGHTS RESERVED.