

OCTOBER 2023

CISA's Evolving .gov Mission

*Defending the United States' Federal Executive
Agency Networks*

AUTHORS

Benjamin Jensen

Devi Nair

Yasir Atalan

Jose M. Macías

A Report of the CSIS Task Force on CISA's Evolving .gov Mission

CSIS

CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

OCTOBER 2023

CISA's Evolving .gov Mission

*Defending the United States' Federal Executive
Agency Networks*

AUTHORS

Benjamin Jensen

Devi Nair

Yasir Atalan

Jose M. Macias

A Report of the CSIS Task Force on CISA's Evolving .gov Mission

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2023 by the Center for Strategic and International Studies. All rights reserved.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

The authors express profound appreciation to Brandon Valeriano, Michael Daniel, Sean Plankey, Moshe Schwartz, Nanni Riddick, Christine Brazeau, and Divya Ramjee. In addition, we would like to thank all of the tabletop exercise participants, especially Chris Inglis and Mark Montgomery, for their contributions.

This report is made possible through the generous contributions of Gray Space Strategies.

About the CSIS Task Force on CISA's Evolving .gov Mission

The Center for Strategic and International Studies (CSIS) conducted a six-month study assessing the cybersecurity services offered by the Cybersecurity and Infrastructure Security Agency (CISA) to federal civilian executive branch (FCEB) agencies. One of the primary roles of CISA is to “provide baseline security” for FCEB agencies and “help these agencies manage their risk.” Recognizing CISA’s critical role in protecting federal networks, this project aimed to answer the following basic research questions:

1. What is the state of current cyber services offered to FCEB agencies?
2. What additional services should CISA plan to offer to protect federal networks more effectively against current threats?
3. What are some of the greatest threats to network security three to five years from now, and will CISA’s current or planned cyber initiatives for FCEB agencies sufficiently protect networks from these future challenges?

To answer these questions, the CSIS team conducted independent research and interviews with public and private sector experts (including a number of current and former CISA program officers). To gain additional insights, CSIS hosted six expert tabletop exercises—and launched an adapted version of the exercise as a public survey—to test assumptions around future challenges and CISA services. An independent task force provided strategic direction to the research team at various stages of the research effort.

The task force consisted of a mix of public and private sector leaders that have all either formally worked in or worked closely with CISA. Each member maintained an enduring commitment to find creative ways of securing cyberspace, with a particular focus on non-defense and intelligence agencies within the FCEB landscape. The following experts served as members of the task force:

- **Suzanne Spaulding (Cochair)**, Senior Adviser for Homeland Security, CSIS; Former Commissioner, U.S. Cyberspace Solarium Commission; Former Undersecretary, Department of Homeland Security
- **Emily Harding (Cochair)**, Deputy Director, International Security Program, CSIS
- **Marene Allison**, Former Chief Information Security Officer, Johnson & Johnson
- **Malcolm Harkins**, Chief Security & Trust Officer, Epiphany Systems; Former Chief Security & Privacy Officer, Intel
- **James Andrew Lewis**, Senior Vice President, Pritzker Chair, and Director, Strategic Technologies Program, CSIS

- **Dr. Phyllis Schneck**, Vice President and Chief Information Security Officer, Northrop Grumman; Former Deputy Undersecretary, Department of Homeland Security
- **David Simon**, Global Co-Head of Cybersecurity & Data Privacy, Skadden, Arps, Slate, Meagher, & Flom; Former Chief Counsel for Cybersecurity and National Security, U.S. Cyberspace Solarium Commission
- **Mark Montgomery (Red Team)**, Executive Director, CSC 2.0; Former Executive Director, Cyberspace Solarium Commission; Rear Admiral, U.S. Navy (Retired)

The task force was led by an executive director and supported by a research team. Further members included the following individuals:

- **Dr. Benjamin Jensen (Executive Director)**, Senior Fellow, CSIS; Professor of Strategic Studies, Marine Corps University School of Advanced Warfighting; Former Senior Research Director, U.S. Cyberspace Solarium Commission
- **Devi Nair (Research Director)**, Former Associate Director and Associate Fellow, International Security Program, CSIS
- **Jose M. Macias (Researcher)**, Research Associate, CSIS; Pearson Fellow, University of Chicago
- **Yasir Atalan (Researcher)**, Graduate Fellow, Center for Data Science, American University
- **Nanni Riddick (Researcher)**, Intern, CSIS

For more information about the CSIS Task Force on CISA's Evolving .gov Mission, see <https://www.csis.org/news/csis-launches-task-force-cisas-evolving-gov-mission>.

Abbreviations

AI - Artificial intelligence

BOD - Binding operational directive

CADS - Cyber Analytics and Data System

CDM - Continuous diagnostics and mitigation

CFAA - Computer Fraud and Abuse Act

CIO - Chief information officer

CIRCA - Cyber Incident Reporting for Critical Infrastructure Act

CISA - Cybersecurity and Infrastructure Security Agency

CISO - Chief information security officer

CNCI - Comprehensive National Cybersecurity Initiative

CNMF - Cyber National Mission Force

CSC - Cyberspace Solarium Commission

CSIS - Center for Strategic and International Studies

CSRB - Cyber Safety Review Board

DHS - Department of Homeland Security

DOD - Department of Defense

DODIN - Department of Defense Information Networks

DOJ - Department of Justice

EO - Executive order

eVRF - Extensive Visibility Reference Framework

FBI - Federal Bureau of Investigation

FCEB - Federal civilian executive branch

FISMA - Federal Information Security Management Act

IP - Internet protocol

IT - Information technology

JCDC - Joint Cyber Defense Collaborative

JCE - Joint Collaborative Environment

JFHQ-DODIN - Joint Force Headquarters - Department of Defense Information Network

KEV - Known exploited vulnerabilities

LANL - Los Alamos National Laboratory

LBL - Lawrence Berkeley Labs

ML - Machine learning

MIT - Massachusetts Institute of Technology

NCWES - National Cyber Workforce and Education Strategy

NDAA - National Defense Authorization Act

NPPD - National Protection and Programs Directorate

NIST - National Institute for Standards and Technology

NSA - National Security Agency

NSF - National Science Foundation

OMB - Office of Management and Budget

ONCD - Office of the National Cyber Director

OT - Operational technology

SCuBA - Secure Cloud Business Applications

SEC - Securities and Exchange Commission

SLTT - State, local, tribal, and territorial

SMB - Small and medium business

SRMA - Sector Risk Management Agencies

ZTA - Zero trust architecture

Foreword

By Benjamin Jensen

This project is about service. It brings together a unique mix of public and private sector voices that cut across industries, political parties, and generations. There are lawyers, soldiers, professors, law enforcement professionals, and former senior appointees and intelligence officers. This diverse group is held together by a commitment to securing cyberspace as a public common where people from all walks of life can prosper.

The members of the task force and research team see twenty-first-century service as helping democratic governments protect the right of free people to exchange goods and ideas through digital networks. Economic, social, and political worlds exist within cyberspace, and the U.S. government has a special obligation to protect them all. These same networks also form key pathways for the provision of the public goods and services that support modern life.

Over 100 agencies comprising the federal civilian executive branch (FCEB) rely on cyberspace to execute their critical functions.¹ That means that over 330 million people in the United States rely on cyberspace for more than social media. They rely on it for basic services such as food and housing assistance. They rely on it for processing student loans. They rely on it for registering patents and starting new businesses. And they rely on it for supporting research labs that are working on new vaccines and clean energy breakthroughs.

A commitment to help develop new strategies for securing cyberspace is what brought the members of this project's task force and research team together. Many have worked on finding ways to balance liberty and security in cyberspace since the 1990s. In 2019, members worked to shape the John S. McCain National Defense Authorization Act and the creation of the U.S.

Cyberspace Solarium Commission (CSC).² Those core members served on the CSC and CSC 2.0 and developed a total of 116 recommendations. Many of these recommendations have either already been implemented, such as the creation of the Office of the National Cyber Director (ONCD), or are nearing implementation.

Still, the job was not finished. In 2022, Cory Simpson—the former lead for helping the CSC think about future and emerging threats—started a dialogue with a network of businesses and senior U.S. government officials on the challenge of securing the FCEB agencies. Based on the new offices and laws recommended by the CSC and ultimately implemented by Congress and the executive branch, along with key executive orders such as May 2021’s Improving the Nation’s Cybersecurity and the 2023 National Cybersecurity Strategy, there was significant momentum to protect the provision of public goods.³ At the same time, daily new reports of massive data breaches, ransomware attacks, and threats of using cyberspace to hold Americans hostage during a conflict with China have revealed the magnitude of the challenge ahead. As the CEO and founder of Gray Space Strategies, a strategic advisory firm, Simpson heard from both government officials and private sector firms that they still felt vulnerable.

This dialogue prompted him to work with Booz Allen Hamilton to reimagine federal network security and resilience. With its support, Gray Space Strategies hired a network of academic and policy researchers to study the balance of threats to federal networks outside of defense and intelligence agencies. The team conducted interviews and mapped out the history of cybersecurity initiatives. As part of this larger research effort, Gray Space Strategies reached out to Solarium alumni at the Center for Strategic and International Studies (CSIS) and sponsored the creation of an independent task force that led to this study.

The net result is in the following pages. The task force and research team built on the work of Gray Space Strategies and conducted over 30 interviews with a mix of federal and private sector chief information security officers (CISOs) and other technical and policy professionals who work every day behind the scenes to deliver public and private goods through cyberspace. Based on these interviews and baseline research, the research team developed a tabletop exercise to illuminate future threats almost certain to challenge FCEB agencies in the near future. Through six expert tabletop exercise sessions held in the summer of 2023 and a parallel online version with 1,000 members of the U.S. general public, the research team was able to see how both experts and the populace see future threats and assess the capability and capacity of the U.S. government to secure cyberspace.

What the task force and research team found is that increasing resources is necessary to meeting the challenge at hand, but it is insufficient. The U.S. government has increased funding for cybersecurity and created new agencies and authorities but still struggles with resourcing strategies that align budgets against risks. The good news is that new initiatives and funding are extending the ability of key players in the federal government to secure the FCEB landscape. The bad news is that processes and procedures still need to catch up to create unity of effort. And time is not on the United States’ side.

Adversaries see better returns from attacking the United States through cyberspace relative to the cost and risk of a more direct confrontation. Perversely, it is easier for them to target critical infrastructure and the basic goods and services offered by the U.S. federal government than it is to shut down the Pentagon or hunt spies online. There is an increasing chance that a major geopolitical crisis becomes a form for digital hostage-taking, with authoritarian states seeking to disrupt FCEB agencies as a way of signaling the risks of escalation to U.S. politicians and the public. This logic flips decades of strategy on its head and makes countervalue targeting—holding innocent civilians at risk—the preferred gambit for authoritarians. The old logic of focusing on counterforce targeting and narrowing hostilities to military forces to preserve space for diplomacy and avoid a broader war may be starting to crumble.

In other words, cybersecurity is not just about force reassurance and protecting defense and intelligence assets during a crisis. It comes down to people. Denying adversaries the ability to hold Americans hostage in cyberspace is now a core national interest. Unlike traditional threats, this denial strategy is not owned by generals and appointees in the Pentagon. It is coordinated by the ONCD and executed by a mix of federal agencies and private sector companies still working to align their priorities and budgets to secure cyberspace.

At the center of this strategy is the Cybersecurity and Infrastructure Security Agency (CISA) and its evolving mission to make civilian government networks (i.e., .gov websites) more secure and resilient. New funding and authorities envision continuous diagnostics and mitigation (CDM) applications standing watch across the .gov ecosystem. These guards are extensions of a complex web of agencies, including the National Institute of Standards (NIST), the Office of Management and Budget (OMB), and the ONCD, all working to coordinate security priorities, technology standards, and budget submissions. On the ground, each FCEB agency has a chief information security officer (CISO) constantly negotiating with their agency leadership about imposing cyber hygiene measures and gauging how much money to dedicate to purchasing approved CDM applications and other cybersecurity efforts. Put simply, each of these agencies has to budget both for defending against national security risks and for their statutory requirements to provide unique goods and services. They face rising costs and uneasy choices given the labyrinth of new resources and authorities coming online. In other words, they need help.

And service starts with helping those most in need. In the pages that follow, the task force and research team offer a list of recommendations intended to start a broader dialogue between the branches of government and the U.S. people about how best to defend cyberspace. **The report is intended to serve as the start of a dialogue about how to best align ends, ways, and means.** The strength of a democracy is its willingness to solve problems in the public square through debate. It is the task force's hope that the recommendations below contribute to ongoing discussions around how CISA in particular can play a useful role in securing cyberspace.

Contents

Executive Summary	1
Introduction	3
How Did We Get Here?	8
<i>Major Incidents, Cyber Strategies, and Legislative Action Pre-CISA</i>	9
<i>The Creation and Empowering of CISA over Three Administrations</i>	12
<i>The Past Is Prologue</i>	16
The Current State	18
<i>Risk Assessment and Vulnerability Management (Pre-incident)</i>	19
<i>From EINSTEIN to CADS</i>	19
<i>Information Sharing</i>	26
<i>Incident Response</i>	30
<i>Resilience Building</i>	31
<i>Training and Exercises</i>	31
<i>General Gaps</i>	34
Future Threats and Challenges on the Horizon	40
<i>Reflections from Expert Interviews</i>	41
<i>Reflections from Tabletop Exercises and the Public Survey</i>	43
<i>Other Challenges</i>	50
Recommendations	55
<i>Pillar 1: Resourcing toward Success</i>	56
<i>Pillar 2: Leveraging and Harmonizing Authorities</i>	58
<i>Pillar 3: Enhancing Communication and Coordination with Key Stakeholders</i>	62
<i>Other Ideas</i>	65
The Future of Collective Defense	68
About the Authors	70
Endnotes	72

Executive Summary

Over the last 40 years, the United States has made progress in securing cyberspace, but its federal networks remain vulnerable to attacks by state and non-state actors. Malign actors can hold the United States hostage by disrupting the ability of the federal government to provide basic services and public goods the country relies on for everything from food to economic growth to cutting-edge research. Beyond the battlefield, the “.gov”—federal civilian executive branch (FCEB) agency—networks remain a critical requirement for American prosperity as well as a crucial vulnerability. Absent renewed efforts to secure these networks, the United States will remain at risk of cost imposition and political warfare in cyberspace.

To address this challenge, the Center for Strategic and International Studies (CSIS) formed a task force of former senior appointees, cybersecurity experts, and private sector chief information security officers (CISOs) to study the past, present, and future of securing the .gov. After a six-month study that involved interviews with federal and private sector CISOs, six tabletop exercises, and a survey of 1,000 members of the general U.S. public, CSIS found that resources alone were insufficient to address the magnitude of the challenge. The U.S. government needs better planning frameworks and coordination mechanisms to work across the diverse mix of agencies within the federal executive branch. Actors such as the Cybersecurity and Infrastructure Agency (CISA) play a leading role but need to find ways to better leverage existing authorities to coordinate resources and risk management across over 100 federal executive agencies. As long as these agencies maintain separate budgets and personnel for managing cybersecurity, it creates inherent planning and coordination challenges. While new reporting requirements and capabilities are coming online, for continuous diagnostics and mitigation (CDM) and threat hunt, the mission to secure the .gov is not

finished. Planning and new response frameworks will need to follow that enable a more robust and fully staffed CISA to work alongside the CISOs in over 100 federal executive agencies to safeguard American prosperity. This long-term planning must include coordinated budgets and strategy with agencies and other key actors such as the Office of Management of Budget (OMB) and the Office of the National Cyber Director (ONCD) alongside synchronizing incident response across the whole of government.

Based on this study, the task force recommends changes to how the U.S. government resources cybersecurity, executes existing authorities, and creates opportunities and incentives to coordinate across over 100 federal executive agencies. Put bluntly, money is not enough to defend the .gov. The U.S. government needs to do a better job of planning, coordinating, and communicating the risks associated with cyberattacks against federal executive agencies. This will likely require consistent staffing at CISA and exploring new service models such as creating collaborative planning teams that deploy to help agencies develop cyber risk strategies and tailored dashboards to monitor their networks.

At the same time, the study surfaced ideas about a number of more contentious but important reforms that warrant further debate. First, the ability of the federal government to attract, train, and retain cybersecurity professionals is a national security issue. Until agencies such as CISA are fully staffed and the federal government has a larger cyber workforce, the ability to defend the .gov is diminished. Second, emerging capabilities like artificial intelligence (AI) and machine learning (ML) have the potential to revolutionize cyber defense but also to create new threat vectors. Agencies such as CISA will have to work alongside current AI/ML strategy efforts to ensure the .gov is ready for an entirely new character of cyberspace. Third, there could be a larger economy of scale to pooling cyber defense resources across federal agencies and creating a more centralized defensive strategy similar to the evolution of the Department of Defense Information Networks (DODIN). Finally, inflation has the potential to complicate resourcing for cybersecurity. Long-term planning efforts will have to ensure that there are mechanisms in place to adapt to sudden changes in prices associated with updating CDM and threat hunt capabilities.

Introduction

Despite over 40 years of investments and initiatives by the U.S. federal government, cyberspace remains vulnerable. Every day brings small intrusions and insidious espionage campaigns designed to hide malware in networks, creating a dangerous complacency that risks the ability of the federal government to provide basic goods and services. Since no single attack has been a major catastrophe capable of competing with stories about war, inflation, public health, and climate change, headlines prove fickle. The money and data that are lost fail to shock the public. Every additional dollar authorized by Congress to protect the network is squeezed by competing requirements. Everyone moves on to the next attack more vulnerable than before.

This tragedy is perfectly encapsulated by the 2020 compromise of the SolarWinds software update, which reveals the promise and peril on the horizon as the U.S. government seeks to secure cyberspace for its citizens.⁴ In December 2020, cybersecurity firm FireEye detected a supply chain attack on SolarWinds' Orion software. The "trojanized" (disguised) malware was unintentionally pushed out to approximately 18,000 federal and private sector clients during a routine software update.⁵ The attack hit nine federal agencies and over 100 private companies, embedding backdoors designed to exfiltrate data—and, in a future crisis, to launch crippling cyberattacks.⁶ Subsequent reporting estimated that the attackers—linked to Russian intelligence—likely had gained access as much as six months earlier.⁷ To put that in perspective, while the National Security Agency (NSA) and Cyber Command proclaimed success in defending forward during the 2020 presidential election and in disrupting Russian cyber capabilities, hackers connected to Moscow were launching one of the largest cyber espionage campaigns in modern history.⁸

At the same time, the SolarWinds response showed the importance of creating a focal point for coordination between the federal executive branch and the private sector, highlighting why twenty-first-century security goes beyond the military and intelligence community. During the SolarWinds crisis, the Cybersecurity and Infrastructure Agency (CISA) worked with FireEye and Microsoft—whose software infrastructure was targeted—to get electronic copies of infected servers.⁹ These copies helped the NSA and Cyber Command diagnose the extent of the malware infection.

The crisis also illustrated the need to accelerate initiatives to secure soft targets across the 102 entities comprising FCEB agencies.¹⁰ In the wake of SolarWinds, CISA has worked to modernize EINSTEIN, a legacy network of sensors on the federal network; create a new Cyber Analytics and Data System; and enhance its Continuous Diagnostics and Mitigation (CDM) program capabilities. These efforts consist of a mix of contracts worth over \$400 million and a request for almost \$500 million in the FY 2024 budget.¹¹ Another effort was the American Rescue Plan Act, which included \$650 million targeted at addressing FCEB agency weaknesses revealed in the SolarWinds and Microsoft exchange intrusions.¹² These efforts are critical to counter evolving threat actors. SolarWinds took an indirect approach and bypassed the EINSTEIN sensors by compromising trusted third-party software.

Resources are necessary but insufficient to protect the over 100 agencies in the FCEB landscape. As seen in SolarWinds, CISA must align resources with strategy and coordinate with diverse stakeholders across the federal government and the private sector to enable entities, public and private, to manage their own risk. Strategy must align ends, ways, and means. Moreover, today's federal cybersecurity has been shaped as much by the threat as by bureaucracy. As such, there is an urgent need to ensure that CISA's security mission is aligned with new offices and authorities—residing in entities including the ONCD—and to overcome defunct dividing lines that characterize how the U.S. federal government buys technology and secures its networks through the various department and agency budget submissions.

Absent a renewed focus on organizational structures and processes within the federal government, the millions of dollars on the table to secure FCEBs will produce diminishing marginal returns. Each congressional dollar appropriated will not produce an equal dollar's worth of security for U.S. citizens. The networks on which the public relies for everything from food and housing subsidies to business permits and patents will prove brittle. As seen with SolarWinds, great powers and other adversaries stand in the shadows ready to exploit the organizational vulnerability of the United States, not just its technical cyber vulnerabilities.

Consider the counterfactual: if the compromise of the SolarWinds software update had not been detected, what could Russia have done to deter U.S. support to Ukraine? The malware pushed to 18,000 federal and private sector networks could have used backdoors to corrupt data and even shut down systems.¹³ Commerce officials could have received false emails with the potential to temporarily distort financial markets. The theft of encrypted keys at the Department of the Treasury could have caused a loss of confidence, not just in financial markets but in the entire U.S. federal tax system. The Department of Energy's National Nuclear Security Administration might have temporarily delayed transporting nuclear materials and operations at multiple national labs, essentially providing Moscow

a nuclear signaling mechanism without an explosion. Department of State correspondence could have been used to mislead U.S. partners as to the nation's willingness to support Ukraine, creating confusion and uncertainty that bought Moscow time to advance on the battlefield.

This counterfactual is not hyperbole. In May 2023, researchers discovered Volt Typhoon, a massive espionage campaign by the Chinese Communist Party to access critical infrastructure networks it could exploit in the event of a crisis with the United States.¹⁴ In addition to targeting U.S. military bases in the Asia-Pacific—home to thousands of service members and their families—the campaign looked for ways to delay troop movements, degrade communications, and cause economic disruption.¹⁵

Military strategy has become fused with cybersecurity as states use cyberspace not just to target armed forces but to hold civilian populations hostage. This digital hostage taking renews the cruel logic of countervalue targeting and threatens to punish civilian infrastructure as a way of limiting an adversary's military options (i.e., deterrence by punishment). Every rail line, airport, or seaport disabled has the potential to delay troop mobilization and create critical supply disruptions that risk public panic. Cyber tools can calibrate the pain, creating a risk strategy in which each vulnerability exploited becomes a signal and pressure for the target to back down or face worse consequences during a crisis.¹⁶ Elected officials in a democracy cannot afford to ignore their citizens, resulting in either capitulation or dangerous escalation spirals.

While the world has yet to see the full use of cyber operations along these lines during a war, states are developing new cyber strategies that integrate coercion, mis-, dis-, and malinformation, and other methods of endangering the modern connectivity the world relies on.¹⁷ The recent Chinese intrusions are a harbinger of a new age of cyber operations. To access networks in Guam, the hackers used internet-facing Fortiguard devices, which incorporate machine learning (ML) to detect and respond to malware.¹⁸ The operation involved using legitimate network credentials and network administrative tools to gain access and develop the ability to launch future attacks. In other words, the attacker used stealth to move with the terrain and find ways of bypassing sophisticated digital sentries.

Even if states like Russia struggled to integrate cyber operations with its military operations in 2022, one should not assume the risk is gone.¹⁹ It is not just AI/ML and generative AI that create new threat vectors in cyberspace. The convergence of digital and critical infrastructure networks opens a new configuration of vulnerabilities across the 16 critical infrastructure sectors (see Figure 1). It is easy to imagine a different type of punishment campaign waged by Moscow that substitutes malware for cruise missiles to attack power plants and key rail lines. Similarly, Russia could have temporarily disabled gas pipelines with cyber operations, a tactic already demonstrated in Saudi Arabia by Iran in 2012.

Figure 1: Cyber Critical Infrastructure Targeting



Source: CSIS International Security Program research.

The number of cyberattacks against critical infrastructure appears to be on the rise. As seen in Figure 1, there is a troubling history of cyber operations targeting critical infrastructure that warrants careful consideration.²⁰ Consider an alternative indirect approach in which a hacker enters through the FCEB agencies linked to these sectors. This is exactly what happened in 2017 when the WannaCry ransomware spread across the National Health Services in the United Kingdom.²¹ In other words, cyber operations targeting FCEB agencies could quickly pass through the federal government and spill over into the broader economy.

Each new device added to a network can improve efficiency but also create emergent risk vectors that would have been unpredictable before its introduction. In 2015, critical flaws were discovered by third-party operational software that connected sensor data distributed across entities such as power plants, water treatment facilities, and pipelines.²² The flaw allowed attackers to execute random SQL statements on the system, in effect enabling hackers to tamper with data, elevate their administrative privileges for future attacks, and conduct denial-of-service attacks. In 2021, 14 of the 16 critical infrastructure sectors in the United States experienced ransomware attacks.²³ This trend continued in 2022, with 140 percent growth in cyber operations targeting the industrial sector (i.e., critical manufacturing).²⁴

As the threat evolves, money alone is not enough to secure cyberspace. The government must adapt and create new ways and means of achieving this common end. This report is part of that effort. The following sections show how the past became the present, helping to frame the challenge facing the different bureaucratic structures and processes used by the federal government to secure non-defense and intelligence functions. Given this historical perspective, the report then pivots to look at the current state, including interviews with senior officials and tabletop exercises with a mix of experts and the general public to understand current threats and challenges. The output of these activities highlights likely futures and how the threat could evolve in the near future. Based on these insights, the report concludes with a list of recommendations on how to align new processes and authorities with resources to protect the resilience of the federal government in the information age.

How Did We Get Here?

New forms of communication tend to produce widespread change.²⁵ As people exchange ideas in new ways, it leads to different social norms, economic revolutions, and challenges to prevailing governance frameworks. And despite modern attention spans, these changes often take a generation to manifest.²⁶

This truth is ever-present in the emergence of the internet and the distributed communications networks that have defined the first decades of the twenty-first century. These modes of communication created new challenges for governing institutions that were accustomed to providing public goods in ways that differed little from the twentieth century. This gap between change and governance created a tension at the core of the federal government.

For decades, it has been increasingly acknowledged within Congress and the larger federal government that there need to be formal mechanisms governing the protection of federal networks. This section provides context for why and how perceptions around federal cybersecurity have evolved, as well as what that means for CISA's mission today.

Seen from a historical perspective, **federal cybersecurity has been shaped as much by threat as by bureaucracy.** From its inception, the internet has seen a combustible mix of great powers and non-state actors competing to exploit network vulnerabilities and hunt the threats that always seem to be one step ahead of the defense. This digital game has strained existing bureaucratic structures and authorities, making it increasingly difficult to coordinate action across branches of government to protect not just cyberspace but the critical infrastructure that is increasingly

reliant on modern connectivity to deliver public goods. These coordination challenges have created planning and budgeting dilemmas that agencies continue to grapple with today.

Looking ahead, federal cybersecurity should be about risk management that aligns to the threat and uses the structure and demands of the bureaucracy to the advantage (not detriment) of cyber defenses.

Major Incidents, Cyber Strategies, and Legislative Action Pre-CISA

FROM BYTES TO RIGHTS: THE EMERGENCE OF CYBERSECURITY REGULATION

Cybersecurity began in the 1970s when researcher Bob Thomas created a computer program called Creeper. Creeper was more an experiment in self-replicating programs than malware.²⁷ It was designed to move between computers and leave a message. Fellow researcher Ray Tomlinson then wrote another program, Reaper, that moved across the early network logging out Creeper wherever it identified the program.²⁸

Great power competition was part of the internet from its inception. By 1981, an independent U.S. federal agency, the National Science Foundation (NSF), had begun several initiatives, dubbed ARPANET, that built off the early internet experiment by the Defense Advanced Research Projects Agency.²⁹ The ARPANET developed the Transmission Control Protocol (TCP) and the Internet Protocol (IP) and set the stage for an NSF initiative connecting computers to create early networks.³⁰ The NSF took on this role because the Department of Defense (DOD) “made it clear they did not want to run a national computer network that wasn’t directly related to defense work.”³¹ One critical NSF initiative was the Computer Science Research Network (CSNET). As the name implies, its goal was to connect computers across national university campuses together.³² The CSNET grew quickly, and by 1981 it merged with the Because It’s Time Network to include email and file transfers.³³ However, the demand for networking grew quickly and set the stage a few years later for joining regional universities with regional supercomputers and the birth of the National Science Foundation Network.³⁴ This critical accomplishment facilitated research, but it also increased opportunities for Cold War rivals such as the Soviet Union and China to conduct espionage on sensitive U.S. data.

From the beginning, however, **threats in cyberspace were not confined to state-based actors.** In 1983, Wisconsin hackers known as the 414s, led by 17-year-old Neal Patrick, breached the computer defenses of the Los Alamos National Laboratory (LANL). LANL was established in 1943 to conduct research for the Manhattan Project and nuclear deterrence. After the FBI investigated the 414s, a congressional report on Mr. Patrick’s witness testimony to a U.S. House of Representative committee highlighted that “ironically . . . [the 414s] gave this new [LANL] account or file the code name ‘Joshua,’ repeating the access code used in the film ‘War Games.’”³⁵ The intrusion into sensitive systems by Mr. Patrick and the 414s highlighted faults in safeguarding computer networks and might have inspired a separate breach in the mid-1980s by agents working for the Soviet Union.

The concept of threat hunt and how best to continuously monitor and defend federal networks has been a central issue since the early days of connected networks. In 1986,

computer managers at the Lawrence Berkeley Laboratory (LBL) discovered a network breach.³⁶ LBL was a university research facility that maintained unclassified research and information on its systems. A 24-year-old hacker based in West Germany penetrated the computer systems at LBL, searching files and emails with keywords such as “nuclear,” “Star Wars,” and “S.D.I. [Strategic Defense Initiative].”³⁷ However, much to the bewilderment of the LBL team, they assessed that this hacker confused LBL with the Lawrence Livermore National Laboratory, a sister laboratory to LBL that conducted classified research.³⁸ In this moment, the team decided to not deny and isolate the intrusion but rather to study it by tracing it back.³⁹ They traced the intruder from multiple points, including a defense contractor in Virginia, a Navy data center, and other military and non-military centers.⁴⁰ The LBL team further alerted and collaborated with the FBI to investigate and eventually charge Markus Hess in 1990 for selling the stolen data for \$54,000 to the Soviet KGB.⁴¹ The character of connected networks enabled easy lateral movement for clever attacks.

For policy practitioners in the cybersecurity field, securing computers was a process that started before the high-profile breaches in the 1980s. An early example is from 1972, when the DOD issued Directive 5200.28, “Security Requirements for Automatic Data Processing (ADP) Systems,” in order to establish “uniform policy, security requirements, administrative controls, and technical measures to protect classified information.”⁴² This directive provided new types of authorities that were built on in 1982 with Directive 5215.1, “Computer Security Evaluation Center,” which established the center at the NSA.⁴³

Planning and standards played a central role early in imagining how to secure networks of connected devices. The two directives mentioned above led to a series of trusted computer system evaluation books published by the DOD and NSA known as the “Rainbow Series,” deriving their name from the colorful covers they were issued in.⁴⁴ The name also paralleled famous U.S. war plans from the interwar period.⁴⁵ The rainbow books were an early attempt to establish standards to secure the DOD components. The most well-known iteration is the “orange book,” published initially in 1983, with a revised version in 1985 titled *Trusted Computer System Evaluation Criteria*.⁴⁶

The defense and intelligence communities were not alone in their efforts to secure computers. Picking up where its response to the 414s left off, Congress introduced a series of bills on computer crimes in the 1980s.⁴⁷ Of the bills introduced, the 1986 Computer Fraud and Abuse Act (CFAA) encapsulated the majority of national efforts to prosecute unauthorized computer network access, codifying civil and criminal penalties and prohibitions against a variety of computer-related conduct and cybercrime. While not exclusively an anti-hacking law, it placed penalties for knowingly accessing a federal computer without authorization.⁴⁸

The first application of CFAA in criminal proceedings came two years later when a modified computer worm resulted in a widespread denial-of-service attack across thousands of computers. In 1988, a computer science student at Cornell University—the son of an NSA official—hacked the computer network at the Massachusetts Institute of Technology (MIT) and planted what became known as the Morris Worm.⁴⁹ This worm did not damage or destroy files, but it quickly slowed down email communications, sometimes for days. While the breach and planting of the worm were at MIT, its fast spread across computer networks caused concern, as even military communications

slowed. As the incident gathered speed and became public, the FBI investigated and eventually charged Robert T. Morris in 1991 for unauthorized access to protected computers. The Morris Worm became the first documented case of the CFAA federally prosecuting a hacker, and it highlighted the importance of protecting cyberspace for the nation.

THE GOVERNMENT BYTES BACK: LEGISLATIVE STRIDES IN CYBERSECURITY

Following the launch of the World Wide Web, Congress continued to work toward improving the resiliency of the federal networks, with a focus on information technology (IT). This came into light in 1995 with the passage of the National Defense Authorization Act (NDAA) and the Information Technology Management Reform Act (Clinger-Cohen Act) of 1995.⁵⁰ The Clinger-Cohen Act was a breakthrough for the federal enterprise because it mandated the creation of chief information officers (CIOs) across agencies.⁵¹ The Clinger-Cohen Act also directed agencies to focus on results using IT investment and streamlined procurement processes, detailing how agencies should approach the selection and management of IT projects.⁵² **Coordinated action by the executive branch and Congress has been central to securing cyberspace for 40 years.**

Building on Congress's actions and picking up the presidential pen in 1998, 10 years after the Morris Worm incident, President Bill Clinton issued Presidential Decision Directive NSC-63. Under the directive, the administration signaled its intent to safeguard cyber-based information systems in critical infrastructure. President Clinton presented five important actions: (1) set a national goal to protect critical infrastructure, (2) appoint agency liaisons to work with the private sector and foster public-private partnerships, (3) create a set of general guidelines, (4) issue structure and organization to federal agencies, and (5) task each agency to be responsible for protecting its own critical infrastructure.⁵³ With the directive, Clinton assured the country that the United States would "take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber-attacks on our critical infrastructures, including especially our cyber systems."⁵⁴ **Early on, federal officials saw the interdependencies between cyberspace and critical infrastructure and between cyber and physical security.**

FROM TERROR TO TECHNOLOGY: THE POST-9/11 CYBERSECURITY OVERHAUL

The very concept of security changed after the terrorist attacks on September 11, 2001. The attacks not only sparked the war on terror but brought the passage of new legislation to safeguard the homeland. Under President George W. Bush, Congress passed the PATRIOT Act of 2001, which amended the CFAA and extended protections to federal computers located outside the United States. Further, the PATRIOT Act also included computers "used by or for a government entity in furtherance of the administration of justice, national defense, or national security."⁵⁵ **New threats showed the need for new authorities.**

In response to both the terrorist attacks and the growing reliance of the federal government on cyberspace, the George W. Bush administration, as a part of its larger Electronic Government (E-Gov) strategy, worked with Congress on the Federal Information Security Management Act of 2002 (FISMA).⁵⁶ The legislation tasked agencies to "identify and provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized

use, disclosure, disruption, modification, or destruction of information systems.”⁵⁷ Importantly, FISMA 2002 not only tasked FCEB agencies with planning out key aspects of their own “tactical-level cybersecurity actions,” but it also attempted to delineate roles between agencies that would support the FCEB agencies, with the OMB providing “strategic support,” the Department of Homeland Security (DHS) providing “operational support,” and the National Institute for Standards and Technology (NIST) establishing standards and guidance.⁵⁸ **The number of agencies involved in coordinating cybersecurity was starting to eclipse the planning and budgeting frameworks in place to manage FCEB agencies.**

In response to these coordination challenges, the White House released the National Strategy to Secure Cyberspace in February 2003.⁵⁹ This strategy was developed in response to the September 11 attacks and set forth the U.S. government’s approach to broadly securing networks, reducing vulnerabilities, and minimizing damage from cyber incidents. It was a whole-of-society strategy, underscoring the importance of public and private entities prioritizing cybersecurity as a way to protect critical infrastructure and processes. With regard to federal entities, the strategy emphasized that the government should serve as a model, leading as early adopters for secure technologies and demonstrating best practices in cybersecurity. Further, the strategy mentioned the importance of developing and maintaining clear roles for federal security management. It cited the OMB’s FY 2002 report to Congress that identified ongoing government security gaps, including but not limited to a lack of attention from senior management, a lack of proper education and general awareness training, a lack of security performance metrics and measurements, and a lack of general ability to detect and share information on vulnerabilities.⁶⁰

The dawn of the twenty-first century saw the United States grappling with new forms of security that eclipsed Cold War-era notions of national security. The active participation of citizens and the provision of goods and services through critical infrastructure emerged as key components that required new thinking. To their credit, officials in the executive and legislative branches rose to the challenge; however, they struggled to achieve lasting results. In the roughly 20 years since the original FISMA and the Bush administration’s National Strategy to Secure Cyberspace, major cyber incidents directly impacting the United States have forced the government to prioritize cybersecurity and reevaluate the very definition of national security. In other words, the proliferation of new networks in cyberspace alongside the acknowledgement that Americans were vulnerable at home drove the need for a new focal point to defend the United States beyond traditional defense, intelligence, and law enforcement considerations.

The Emergence of CISA over Three Administrations

THE OBAMA ADMINISTRATION: PAVING THE WAY FOR CISA

As a continuation and expansion of Bush-era cyber recommendations, the Obama administration and successive congresses struggled to find the best alignment of cyber and critical infrastructure protection within the newly created DHS.⁶¹ **The optimal structures and processes for securing cyberspace remained elusive.** Many of the initiatives built in 2007 realigned multiple agency portfolios on cyber and critical infrastructure—including defending FCEB agencies—under

the National Protection and Programs Directorate (NPPD).⁶² Through such efforts, the Obama administration laid the foundation for what would eventually become CISA within the DHS.

First, the administration conducted a 60-day review of the nation's cyber policies and processes, culminating in the 2009 Cyberspace Policy Review.⁶³ It then developed and published the Comprehensive National Cybersecurity Initiative (CNCI), detailing cybersecurity goals for agencies such as the OMB and DHS. The report was an outgrowth of the CNCI initiative launched by President Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), which called for the federal government to “integrate many of its technical and organizational capabilities in order to better address sophisticated cybersecurity threats and vulnerabilities.”⁶⁴ It also built substantially upon the report of the CSIS Commission on Cybersecurity for the 44th President, *Securing Cyberspace for the 44th Presidency*.⁶⁵ Of relevance to this study, President Obama's CNCI report details initiatives such as the management of a Federal Enterprise Network with Trusted Internet Connections and the deployment of intrusion detection and prevention systems across the federal enterprise. In other words, **policymakers have seen the importance of defending FCEB agencies and the .gov ecosystem for over 20 years but have struggled to align resources to achieve their ends.**

It was also during this time that the DHS started building and improving on a number of initiatives that have since become key services managed and delivered by CISA. For instance, in 2012, the DHS established the Continuous Diagnostics and Mitigation (CDM) program and rolled out EINSTEIN 3 Accelerated, which added inline blocking to existing EINSTEIN intrusion detection.⁶⁶

Separately, after nearly a decade of FISMA 2002 guidelines, the Obama administration signed a new FISMA into law in 2014. In addition to updating and streamlining reporting requirements, the new FISMA further delineated roles and responsibilities in cybersecurity management by formally codifying the DHS's role as the lead for implementing and overseeing FCEB agencies' IT policies. The government saw a need to coordinate technology standards by getting policies aligned.

Most importantly, it should be noted that it was during the final years of the Obama administration that the NPPD was able to develop the plans for the first new operational agency at the DHS since its founding.⁶⁷ This plan was provided to Congress and became the basis for later establishing CISA. At the same time, it was clear that these initiatives were still failing to deliver what they promised: an integrated approach to cybersecurity and risk management across the federal government. As seen in the 2015 OMB hack, FCEB agencies were often late in submitting their cyber strategies and struggled to recruit and retain talent.⁶⁸ This fact led some circles to call for moving cybersecurity out of the DHS and creating a standalone National Cyber Authority.⁶⁹

THE TRUMP ADMINISTRATION: CONSOLIDATING AUTHORITIES AND RESOURCES

Efforts to align federal resources to secure cyberspace accelerated during the Trump administration. Building on President Trump's Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, the administration also released its National Cyber Strategy in September 2018—the first official strategy since the Bush administration's in 2003.⁷⁰

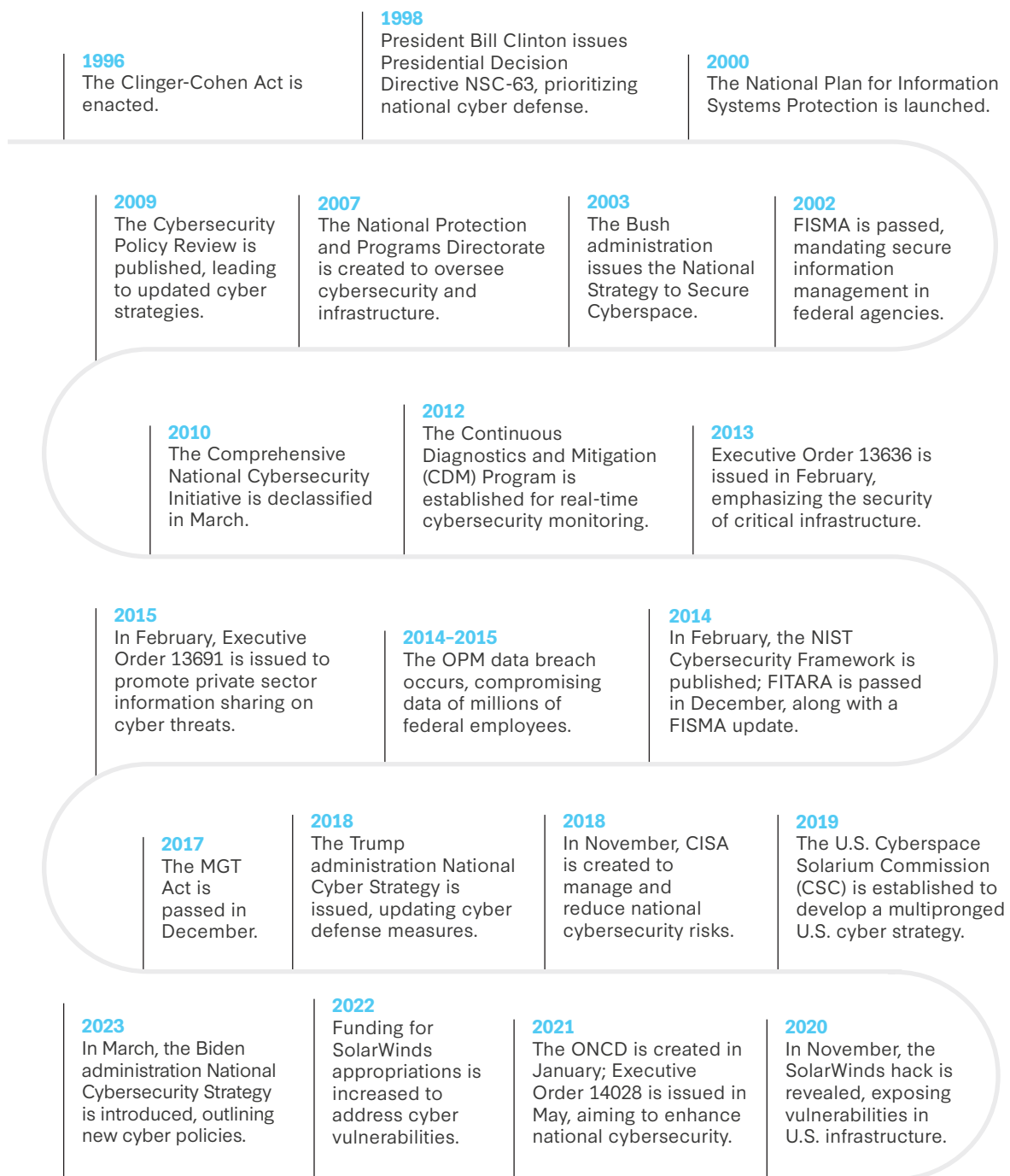
A few months after the release of the 2018 cyber strategy, the Cybersecurity and Infrastructure Security Act was passed and signed into law, formally creating CISA. The creation of CISA isolated, consolidated, and elevated key functions of the DHS's NPPD and related DHS initiatives. While the NPPD was already tasked with the majority of the DHS's cyber responsibilities, this rebranding of the NPPD's cyber offerings to CISA was more than just a way to consolidate efforts. The initiative also started a path toward greater unity of effort. CISA was empowered to carry out its cyber mission as part of DHS's mandate to strengthen the security and resilience of critical infrastructure, including federal civilian networks and mission-essential functions.⁷¹ **The consolidation of resources and authorities can help elevate the mission, but its successful execution relies on buy-in from the clients—in this case, FCEB agencies.** The question remained of how best to align resources with the new agency and ensure that it could work, with FCEB entities scattered across the departments outside of the DHS.

THE BIDEN ADMINISTRATION: SUPPORTING AN EVOLVING CISA MISSION

The Biden administration has continued to build on initiatives started under the Trump and Obama administrations. This continuity relates to the fact that many cybersecurity initiatives involve Congress as much as they do the executive branch. For example, in March 2020, the bipartisan U.S. Cyberspace Solarium Commission published its final report. Notably, two of its key recommendations were to (1) establish a Senate-confirmed national cyber director, and (2) strengthen CISA.⁷² Congress officially established and confirmed a national cyber director, Chris Inglis, in 2021. As one of its primary deliverables, the ONCD developed the Biden administration's National Cybersecurity Strategy in March 2023.⁷³ An implementation plan was further released in July 2023.⁷⁴

The early years of the Biden administration also saw a lot of activity around EO 14028, Improving the Nation's Cybersecurity, and a slew of other executive branch guidance documents supporting and reinforcing it.⁷⁵ Of relevance to this report, EO 14028 directs federal government agencies to adopt zero trust architectures (ZTA), a move that has created a necessary—albeit arguably insufficient—role for CISA as the agency that can provide general guidance to FCEB agencies during their ZTA migration.⁷⁶

Figure 2: U.S. Government Cybersecurity Timeline



Source: CSIS International Security Program.

In recent years, CISA received additional authorities and resources, the details of which are outlined later in this report. It should also be noted that Congress pushed for FISMA reform in 2022.⁷⁷ If passed, the new legislation would have further enhanced CISA's authorities. However, the legislation

passed in the Senate but failed to do so in the House, leaving FISMA 2014 as the status quo. A bipartisan effort is underway to tackle FISMA reform again in 2023. The current bill tracks closely with provisions outlined in the 2022 version (see Recommendation 2.1 in this paper on a report to evaluate CISA's current and future FCEB mission).⁷⁸

In its next stage of growth, CISA needs to invest in and be supported by larger structural and cultural changes that allow the agency to more effectively work as a strategic partner with FCEB agencies to protect federal networks.

The Past Is Prologue

While this section does not provide a comprehensive list of legislative proposals and actions, the selected events and documents represent flashpoints that drove efforts to protect federal networks. Collectively, these events and milestones also paved the way for CISA to assume its important role as the cybersecurity lead for FCEB agencies.

The diffuse and evolving character of cyber threats makes it difficult to galvanize more definitive policy responses. To date, the United States has not experienced a “cyber 9/11” or a “cyber Pearl Harbor.” Instead, the nation has experienced a series of cyber incidents that, while not necessarily small, have captured public attention to a much lesser degree than terrorist attacks. The result is twofold. On one extreme, certain FCEB leaders do not fully appreciate how cyber threats can impact an agency's ability to carry out its mission. On the other extreme, there are policymakers, government leaders, and experts who are overeager to plan for the big cyber incident on the horizon—sometimes at the expense of sufficiently planning for the immediate and persistent “smaller” attacks that, when taken together, can greatly undermine the government's ability to deliver basic services to the American people.

Encouragingly, the past four administrations—in partnership with Congress, the private sector, and state, local, tribal, and territorial (SLTT) governments—have taken great strides to positively elevate cybersecurity, underscore the importance of coordination and collaboration, and at least nod toward the importance of enhancing resilience. But as the threat landscape evolves, so too does the need to create new entities, develop new policies, and adopt new security outlooks and models. While this is generally a welcome trend, without proper coordination or harmonization it can resurface some of the issues identified 20 years ago, such as the need for clearer delineation of cyber leadership roles, and the need for a greater sense of urgency from department and agency leads.

With regard to CISA, it is unequivocally clear that the agency is the operational lead for FCEB cybersecurity, and there is general bipartisan support to enhance CISA's ability to carry out that mission. Logistically, however, there remain a number of questions, including but not limited to: What does it mean for CISA to sufficiently protect an FCEB network? What entities, federal or otherwise, play a formal or informal role in helping CISA protect federal networks? And how much of the security burden should FCEB entities manage on their own versus handing off to CISA?

In September 2022, CISA unveiled its Strategic Plan: 2023-2025—the agency’s first since its creation in 2018—and followed it up in August 2023 with its Strategic Plan: FY2024-2026.⁷⁹ What immediately stands out is that CISA’s mission space is vast and that its role as the leader of FCEB cybersecurity is just one of many hats it wears as the nation’s cyber defense agency. **Moving forward, it will be important that the executive and legislative branches continue to empower CISA in ways that responsibly grow its capabilities, authorities, and resources without overextending or compromising its ability to carry out its mission.**

The Current State

Despite the generational struggle to secure FCEB agencies in cyberspace, there are signs of hope on the horizon. Consider the operations of the National Aeronautics and Space Administration (NASA). Amid all the excitement and chaos surrounding a non-cyber event, a lesser-known operation can be simultaneously underway: a CISA incident response exercise. While it is not ideal to run a network intrusion exercise, what the mission leaders at NASA understand well is that inconvenient times are precisely when an adversary is most likely to attack. Stress-testing responses during real, critical missions is the best way to assess preparedness and system resilience plans. Furthermore, the case shows the art of the possible: agency-level coordination and planning that takes advantage of CDM and threat hunt capabilities.

CISA's cybersecurity services to FCEB agencies are varied. Some, such as its system monitoring and threat hunting initiatives, rely on CISA's technical capabilities. Others, like its ability to run scenario exercises for FCEB entities, rely on the agency's ability to leverage partnerships, relevant expertise, and guidance in ways that can support FCEB agencies' individual plans to secure their respective networks. All require coordination and planning that align agency interests across a diverse set of stakeholders in the FCEB space.

These services have been met with varying degrees of tangible and perceived success. To properly assess current cyber services offered, it is important to evaluate how these initiatives have evolved in recent years and the ways in which FCEB entities actually interact with and utilize them. The non-mutually exclusive categories below underscore some of the primary cybersecurity services that CISA offers to FCEB agencies.

Risk Assessment and Vulnerability Management (Pre-incident)

Arguably some of CISA's most important programs are those that help FCEB agencies gain greater visibility into their networks, allowing them to proactively identify and defend against bad actors on their systems. Over the next few years, this is one area where CISA looks to expand its capabilities, especially as adversaries grow more adept at circumventing traditional cyber defenses.

Visibility and assessment tools can only be effective if they communicate with each other and can collectively provide an accurate, robust, and up-to-date picture of existing vulnerabilities. Since investments in pre-incident detection capabilities are rapidly growing, with the goal of providing more visibility for FCEB agencies and CISA, it is important to assess the state of current services and planned initiatives by asking the following: Are updates being clearly communicated to relevant industry and FCEB partners? Will there be any visibility gaps when moving from older to newer monitoring systems? And do planned activities integrate well with other services offered by CISA? While interviews with and public announcements from CISA representatives indicate that the agency is tracking these questions and looking for ways to facilitate smooth transitions, some outside stakeholders might need further convincing that CISA will not only prioritize data integration but also have the capabilities to do so in a seamless way.

From EINSTEIN to CADS

In its *2022 Year in Review*, CISA noted that it will be sunsetting the legacy EINSTEIN program and building out newer capabilities in its place that are better able to monitor and detect network intrusions.⁸⁰ It will be important for CISA to focus efforts on clearly communicating what aspects of EINSTEIN will continue, what will be improved, and what, if any, visibility or service gaps might arise during transition periods. **The modernization of well-known, well-utilized capabilities like EINSTEIN should be clearly articulated to all stakeholders so as to not unintentionally create new areas of confusion.**

CISA's EINSTEIN program is an intrusion detection system that monitors traffic coming in and out of FCEB networks. The program was initially developed in 2004 by the U.S. Computer Readiness Team and consists of three phases: EINSTEIN 1, EINSTEIN 2, and EINSTEIN 3. Traditionally, FCEB agencies would enter partnership agreements with CISA that essentially allow it to install systems and sensors for collecting information on potential threats to the network. The program operated as an early warning system with "near real-time" awareness of potentially malicious cyber activity.⁸¹ Per an interviewed expert with deep knowledge of the evolution of the program, most FCEB agencies are only aware of the EINSTEIN sensors—the connection points. However, that is only 10 percent of EINSTEIN. There is a larger infrastructure behind the program that collects inputs from a number of other feeds to provide more robust information.

The stated plan is for EINSTEIN's "analytics, information sharing, and core infrastructure" capabilities to shift to CISA's Cyber Analytic and Data Systems (CADS).⁸² This will allow CISA to "more rapidly analyze, correlate, and take action to address cybersecurity threats and vulnerabilities before damaging intrusions occur."⁸³ The overarching concept is for CISA to be

the center of FCEB and critical infrastructure threat intelligence, centralizing this data enables analytics that may identify individual events or the spread of events, which in turn will enable faster detection and notification. For FY 2023, CISA targeted \$91 million of funding to keep its National Cybersecurity Protection System, which is known for its EINSTEIN set of capabilities.⁸⁴ Of the \$1.8 billion requested by CISA for FY 2024 efforts related to its FCEB mission, CISA is requesting approximately \$425 million dollars specifically for CADS.⁸⁵ EINSTEIN 1 and EINSTEIN 2 capabilities will primarily be under the authority of the new CISA CADS team, while CISA's Protective DNS and proposed Protective Email services will serve as a successor to EINSTEIN's 3A capabilities.⁸⁶ The Protective DNS service, distributed across various locations, blocks attempts to access potentially harmful online resources—such as domains or IP addresses—identified by threat data from commercial sources, governments, and agencies. It logs the associated DNS traffic for detailed analysis.⁸⁷ Furthermore, this service complies with the mandate from DHS under Title 6 of the U.S. Code, Section 663, which emphasizes the need to detect and mitigate cyber threats in network traffic.

Ultimately, the creation of CADS is also supposed to support the larger Joint Collaborative Environment (JCE), an “interoperable environment for sharing and fusing threat information, insights, and other relevant data” between and across public and private sectors.⁸⁸ This initiative was first introduced by the CSC, and in recent months CISA has mentioned that it is actively working to build it out, despite no formal direction and funding from Congress (see Recommendation 1.2 on Congress authorizing and funding a JCE).

Given that a mix of programs is already underway, and that others are still up for approval and authorization, it will be incumbent on CISA to provide routine status updates of the transition progress from EINSTEIN to CADS and to offer possible workarounds for any delays.

CIRCIA: Powering CADS with the Right Kind of Information

A key part of CADS is ensuring that quality, comprehensive information is fed into the system. In March 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).⁸⁹ For decades, when critical infrastructure facilities and FCEB agencies were victims of a cyber incident, they were not legally required to report the incident to the federal government. CIRCIA, among other things, tasks CISA to outline cyber incident reporting requirements for “covered entities.” CISA has until March 2024 to publish a Notice of Proposed Rulemaking and then 18 months to publish the Final Rule.⁹⁰ Until this goes into effect, cyber incident reporting is still voluntary—though strongly encouraged—with industry providing feedback on the best way to structure reporting and deconflict with other requirements, including those of the Security and Exchange Commission.⁹¹

To be successful, CISA needs to identify regulations that collect necessary information without placing undue burdens on reporting entities. It must also make sure that new

regulations are harmonized with existing reporting requirements. Relevant to CADS, if CISA is able to structure reporting requirements in a way that goes beyond just notifying the authorities that an incident has occurred but that also captures the technical attributes of an attack, that information can be pulled into CADS at machine speed and provide greater visibility.

CIRCI reporting requirements will bring critical event data into CADS and illuminate events from smaller companies that had not previously been engaged. This thwarts adversary efforts to attack smaller members of the supply chain in the hopes of remaining “below the radar” (see Recommendation 2.2 on reporting requirements).

Increased investments in gathering and analyzing cyber data can increase FCEB network security. First, because the majority of internet traffic takes place on private sector networks, understanding the vulnerability landscape based on incident reporting serves as a form of early warning for the federal government. Investments in CADS that enable machine speed analysis of emerging vulnerabilities and the likelihood of exploitation by different actors empower agency CISOs to manage risk. To be effective, this new data-driven approach to risk analysis will need to ensure proper communication and coordination, as well as a historical inventory of vulnerabilities supporting longitudinal assessments.

CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) PROGRAM

Increasing investments in the technical analysis of cyber vulnerabilities produces a library against which to monitor FCEB agencies. Along these lines, CISA has made the CDM program a central focus of its efforts to ramp up network defense. The Biden administration’s FY 2024 budget requests \$408 million for CDM, an increase from the \$292 million that was appropriated in FY 2022 and the \$332 million appropriated in FY 2023.⁹² Per Michael Duffy, CISA’s associate director for capacity building, it is “the U.S. government’s cornerstone for proactive, coordinated, and agile cyber defense of the federal enterprise.”⁹³ **Given its critical role, it is essential not only that CDM efforts are sufficiently resourced in the coming years, but that there are plans in place for long-term funding so that FCEBs can continue to benefit from the CDM program without disrupting current services.**

Whereas EINSTEIN provides perimeter defense, CISA’s CDM program works within FCEB networks to further enhance overall security. Developed in 2012, CDM provides cybersecurity tools, integration services, and a user-friendly dashboard to FCEB agencies so that CISA can gain greater visibility into FCEB networks.⁹⁴ Many of the core concepts within CDM date back to NIST guidance from 2011 and early experiments by the Department of State and Army Research Lab in support of DOD networks.⁹⁵

Overall, the CDM program engages technologies to identify and protect electronic assets, then displays the status on a dashboard, a bit like a running car will show the activity ranges of its components. It is complementary to EINSTEIN and CADS in that it provides the inner workings of a network while a program such as CADS analyzes perimeter activity for ingress and egress attempts.

The CDM program specifically offers five program areas: (1) a dashboard that receives, aggregates, and displays cyber health at the agency and federal level; (2) asset management to answer the question “What is on the network?”; (3) identity and access management to answer the question “Who is on the network?”; (4) network security management to answer the question “What is actually happening on the network?”; and (5) data protection management. The CDM program then uses data collected through its suite of tools to populate agency-level dashboards to 23 agencies, as well as a federal version.⁹⁶ The agency dashboard is a data visualization tool that produces reports and alerts IT managers to critical cybersecurity risks. The federal dashboard provides a macro-level view that consolidates information from each agency-level dashboard for a better picture of cybersecurity health across all civilian agencies.⁹⁷ Dashboards in turn become an important tool for visualizing and describing risk, a capability that can be further enhanced through migrating to a JCE and longitudinal analysis. The CDM program is an excellent tool for measuring compliance, but far beyond this, it dynamically measures security and risk, enabling a combination of best-in-class tools and metrics to determine success.

CISA advertises that CDM will directly help FCEB agencies by reducing agency threat surface, increasing visibility, improving response capabilities, and providing assistance more generally.⁹⁸ CISA has also issued Binding Operational Directive (BOD) 23-01 which mandates regular, automated reporting to CDM for FCEB agencies.⁹⁹ The impact of BOD 23-01 for CISA and FCEB agencies is significant: by mandating the automation of data, the gains are bidirectional. Where CISA gains further visibility into the federal enterprise, so do FCEB agencies, helping them both manage risk in their operations and tailor responses such as patching or threat hunting.

With the new authorities granted to CISA in the FY 2021 NDAA, CISA no longer needs formal agreements to actively carry out threat hunting on FCEB networks.¹⁰⁰ Acquiring those formal agreements consumed valuable time that delayed incident response. Even as recently as a few years ago, CISA had to heavily rely on voluntary security reports from FCEB agencies. Now, new authorities coupled with new endpoint technologies allow CISA to view and collect object-level data across FCEB networks and to produce instantaneous threat reports that match the pace of adversary activity. At the same time, the technical ability to hunt on an agency network does not usurp requirements for collaborative planning and risk discussions. While CISA is making technical strides, the area it needs to refine is how best to leverage network access and a common operating picture to support risk management across the FCEB landscape. **Technology absent planning is subject to diminishing marginal returns** (see Recommendation 1.1 on consistent funding streams).

Two Is Better Than One

CISA director Jen Easterly described the power of CADS and CDM in a congressional hearing as the following: “Together . . . these programs provide the technological foundation to secure and defend FCEB departments and agencies against advanced cyber threats. CDM enhances the overall security posture of FCEB networks by providing FCEB agencies and CISA’s operators with the capability to identify, prioritize, and address cybersecurity threats

and vulnerabilities, including through the deployment of Endpoint Detection and Response (EDR), cloud security capabilities, and network security controls.”¹⁰¹

In many ways, CISA’s CDM program is good news. CISA reported in its FY 2023 Q2 update that 55 percent of federal agencies automatically report to CDM.¹⁰² This means they have already surpassed their goal of getting half of all agencies to automate reporting by the end of the fiscal year.¹⁰³ Additionally, a 2022 MeriTalk survey of federal and industry stakeholders reported that 93 percent of respondents believed that CDM had improved federal cyber resilience in several ways, with 84 percent noting that CDM actively helped entities comply with EO 14028 requirements.¹⁰⁴ These sentiments seem consistent with those of the experts interviewed for this project. However, in that same MeriTalk survey, only 28 percent of respondents gave CDM an A grade, with responses to other questions demonstrating a belief that CDM is a compliance-based activity (rather than a risk management activity) and that it has a way to go before it reaches its full potential (see Recommendation 2.7 on CDM after-action reviews).

The biggest problem, however, is that the CDM funding model is not ideal and that agencies have yet to develop a common risk planning framework tied to resources. Currently, CDM is structured so that CISA covers the initial cost of required tools for two years, after which the FCEB agencies are required to pay for their continued use and maintenance by themselves. There are reasonable concerns that some FCEB agencies are not able or willing to sufficiently budget for the continued use of these tools. Setting aside general inflation-related cost increases, FCEB agencies might not be appropriately factoring into their budget plans the outyear costs for CDM. Current and former CISOs interviewed by CSIS expressed that vendors are closely monitoring these deadlines and coming back to FCEB agencies with tools that are cheaper than the ones that agencies might currently be using but that are not necessarily as capable. As one expert noted, “there’s a lot of chum in the water,” and the situation is difficult for some FCEB agencies to navigate. There are major security concerns as well: CISA invests time and resources to help agencies integrate specific tools, so when those FCEB entities switch to alternatives, CISA might lose progress or visibility for a set period of time as those new tools are integrated into the network—assuming they are ever properly migrated to the CISA dashboard.

CISA is in a difficult position. As one expert interviewee acknowledged, CISA is managing expectations and has been generous in its time and general efforts to stand up these programs with FCEB agencies. The general funding model is not ideal, but it also cannot provide guarantees of financial support beyond a set period of time.

The net result is that CDM has made strides in monitoring over half of the FCEB agencies, but the future is clouded by complex bureaucratic and budgeting questions. Even if an agency can resource CDM after the initial two-year window, it struggles to forecast how much it will cost and is confronted with a labyrinth of rules surrounding which congressionally approved budget vehicles and authorities it can use to essentially “buy” security (see Recommendation 1.1 on properly resourcing CDM). In other words, beyond CDM, CISA will need to develop planning frameworks that

help align resources against risk assessments and competing budgetary requirements, alongside other actors such as the ONCD and OMB. The federal government cannot buy cybersecurity off-the-shelf products alone to solve the problem. It needs to revisit how it plans and manages resources related to securing networks across FCEB agencies (see Recommendation 2.9 on risks that accompany FCEB budget strategies) as well as how to create dashboards agencies can tailor to monitor their networks.

At the same time that NIST moved to standardize information security continuous monitoring, the cybersecurity community started to hypothesize a coming paradigm shift. Rather than being the “hunted,” constantly responding to threats after they turned into incidents on the defended network, the CISO would become the “hunter.”¹⁰⁵ The concept relates to a practice in the early 2000s by U.S. Air Force personnel, who used the term “hunter-killer” to describe teams of cybersecurity experts conducting force protection on their networks.¹⁰⁶ The term evolved to describe how senior cybersecurity experts would train new analysts by taking them on “hunting trips.”¹⁰⁷ Many of these practices paralleled the rise of using more active red teams to test network defense, as well as a new focus on advanced persistent threats in the cybersecurity community to describe more robust government-sponsored threats.

In practice, the move from CDM to threat hunt will likely involve more than just purchasing new software. From its origin, the practice involved a mix of red-teaming exercises that connected discrete events across a data sample on possible vulnerabilities. That is, similar to the process envisioned by the JCE, the process requires a repository of data—including common coding typologies such as MITRE ATT&CK—to be effective, along with a mix of collaborative planning and exercises to emulate adversary actions.¹⁰⁸ Threat hunting is as much a practice and an art as it is a technical science.¹⁰⁹

CDM Enables the Hunt

CISA is making progress on threat hunt and can accelerate it by serving as a central coordinator for threat hunt across FCEB agencies. For example, in March 2023, CISA released Decider, a collaborative tool designed to help agencies map risk using the MITRE ATT&CK framework.¹¹⁰ The tool is an example of the need for a larger array of common planning and collaborative tools across the FCEB landscape, many of which need not originate in but should ultimately be coordinated by CISA. Along these lines, CISA worked with Sandia Labs to deploy to the Untitled Goose Tool in March 2023, which specializes in authenticating and analyzing data linked to cloud services.¹¹¹

FEDERAL CLOUD SECURITY

As more FCEB agencies rely on the cloud for their activities, it creates new vulnerabilities. To that end, EO 14028 directs CISA to support efforts to modernize security standards across the federal network. The resulting cloud strategy provides a shared understanding of security standards,

configurations, and visibility requirements. **But providing the framework is different than actively supporting the implementation of processes and technologies that FCEB agencies might adopt to comply with the guidance.**

This strategy works alongside the larger process involving NIST, the General Services Administration, the DOD, and the DHS to standardize approaches to securing cloud computing consistent with the original vision in FISMA 2002 and 2014.¹¹² The goal is to balance rapid deployment of cloud computing with sufficient security standards and protocols.¹¹³ FCEB CISOs select from a list of approved software vendors (i.e., software-as-a-service) that as of the spring of 2023 totaled 300 cloud service offerings.¹¹⁴ The result is a calibrated, risk-based approach to secure cloud services adoption across the federal government by providing standards for cloud services and facilitating a partnership between the federal government and private industry. In addition to long-term cost saving, this approach is intended to save time for agencies and industry providers alike by having everyone operate off a shared security framework.

CISA goes one step further by providing additional guidance to and support for FCEB agencies, advising them on how to actually adopt secure cloud products. Among its prominent initiatives, CISA has introduced the Extensive Visibility Reference Framework (eVRF) and the Secure Cloud Business Applications (SCuBA) project.

SCuBA focuses on securing cloud business applications, providing security guidance through the SCuBA Technical Reference Architecture that is closely aligned with zero trust principles. This architecture offers context, standard views, and threat-based guidance for secure cloud business application deployments, and it aims to secure the cloud environments where federal information is created, shared, and stored. Agencies are expected to cooperate with CISA by implementing comprehensive logging and information-sharing capabilities for better visibility and response to cloud threats.

The architecture document, acting as the foundational guide for the SCuBA program, offers a vendor-agnostic approach to securing business applications, aligning with zero trust principles. The eVRF guidebook, on the other hand, helps organizations identify data visibility gaps and provides strategies to mitigate threats. eVRF encourages agencies to provide necessary data to CISA. The agency then evaluates the FCEB agencies' visibility capabilities and helps integrate visibility concepts into their FCEB cyber practices.

What might be helpful moving forward is for CISA to assess how FCEB agencies are engaging with these materials. For example, are they actively being used to develop agency specific plans? Are they adequately filling information gaps that currently exist across FCEB agencies? And do FCEB entities require additional training aids or materials to better assist with implementation?

These questions are all the more critical given recent audits of FedRAMP compliance across FCEB agencies and the announcement of forthcoming FedRAMP guidance that will address advancements in the cloud marketplace.¹¹⁵

Information Sharing

One of CISA's value propositions in the federal government is its ability to engage with the private sector. What that means for FCEB agencies is that information-sharing programs hosted and facilitated by CISA valuably pull not only from other government entities but from a number of private sector organizations as well. The key aspects of information-sharing services that can be measured and evaluated include (1) quality of information, (2) timeliness of shared information and updates, (3) reach of information sharing, and (4) format of outputs. While CISA has made gains across these metrics through creating vulnerability catalogs and collaboration environments, it is struggling to keep up with the magnitude of the current cyber threat.

Another key value that CISA uniquely brings is the ability to create a ConOps, or an overall cyber threat picture, populated by real-time activity reports from across FCEB agencies and critical infrastructure. No other entity can do this—not even cybersecurity vendors—once critical infrastructure events are reported into CISA and CDM dashboards are lit up. This is a unique tool and a huge “shields up,” since cyber adversaries cannot assemble this picture. But the United States must follow the steps necessary to gain this advantage: creating the apparatus and expediting cooperation, reporting events, and disseminating threat intelligence back out to FCEB agencies and industry.

KNOWN EXPLOITED VULNERABILITIES CATALOG

CISA's BOD 22-01 mandates that FCEB agencies mitigate known exploited vulnerabilities (KEVs) in their systems.¹¹⁶ The BOD established the Known Exploited Vulnerabilities Catalog to list computer Common Vulnerabilities and Exposures and require agencies to remediate vulnerabilities within specific deadlines—15 calendar days for high or critical severity vulnerabilities and 30 calendar days for medium or low severity ones. Agencies are responsible for reviewing the catalog daily, notifying CISA of any barriers to compliance, and submitting regular status reports. The KEV catalog was mentioned in a number of interviews as a valuable CISA resource. Ongoing success will rely on continuing to receive and provide updates in a timely manner, as well as on FCEBs properly understanding how to act on and prioritize the information presented in the catalog.

The KEV catalog recently reached 1,000 entries.¹¹⁷ Its intent is to help organizations prioritize vulnerability management efforts, with several major vendors integrating KEV data into automated vulnerability and patch management tools.

Binding Operational Directives

From time to time, the DHS will issue Emergency Directives and Binding Operational Directives (BODs), compulsory mandates that direct departments and agencies to take certain actions that will help them safeguard their systems. The DHS is authorized to do this through CISA per FISMA.¹¹⁸ While this is not a CISA service per se, the development, rollout, and enforcement of BODs play a key role in supporting CISA's larger federal network defense mission.

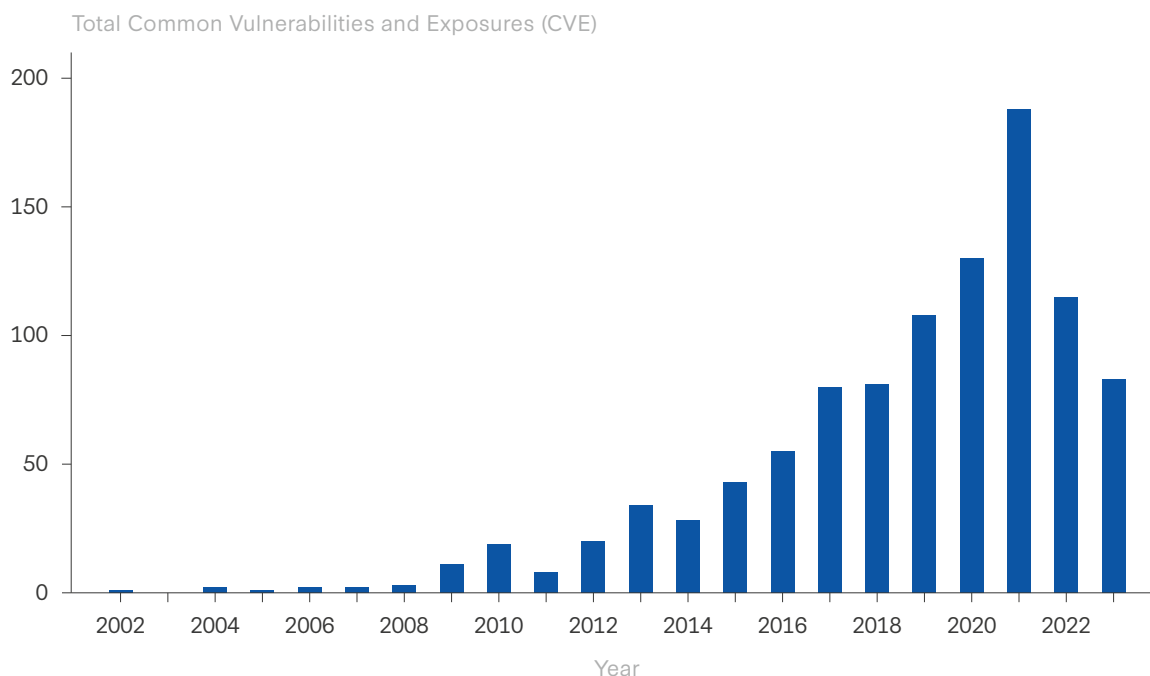
The following are some of the more recent and relevant BODs impacting FCEB network defense:

- BOD 23-02: “Mitigating the Risk from Internet-Exposed Management Interfaces”;
- BOD 23-01: “Improving Asset Visibility and Vulnerability Detection on Federal Networks”;
- BOD 22-01: “Reducing the Significant Risk of Known Exploited Vulnerabilities”; and
- BOD 18-02: “Securing High Value Assets.”

Beyond general information about the vulnerabilities themselves, the KEV catalog also captures other important trends with implications for broader cybersecurity. For instance, over three-quarters of the updates in the KEV catalog relate to older vulnerabilities, suggesting the persistence of long-standing security risks across agencies. Likewise, it could also be that vulnerabilities may exist in the wild but have not been optimized to do harm. The inclusion of end-of-life systems, such as Windows Server 2008 and Windows 7, indicates that there are still many organizations utilizing legacy systems.

However, further review of the catalog reveals that it would sometimes take over a week after public disclosure for a vulnerability to be added to the catalog. The KEV catalog is not meant to serve as an early warning system. It is a problem that some entities perceive and use it that way.¹¹⁹

Figure 3: CISA Known Exploited Vulnerabilities 2023



Source: “Known Exploited Vulnerabilities Catalog,” Cybersecurity and Infrastructure Security Agency, accessed August 21, 2023, <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.

Moreover, while the information from the KEV list is definitely useful, one of the interviewed federal experts noted that it would be even more helpful if the catalog clearly distinguished differences between the listed vulnerabilities. For example, if CISA pushes an updated list with 10 new entries, are there certain vulnerabilities that federal CISOs should be most concerned about and should address first? Are there others that are lower on the priority list? Moving forward, the catalog's usefulness will be graded on its ability to update information in a relatively quick manner, while also clearly communicating to users how they should interpret and act on listed information.¹²⁰

JOINT CYBER DEFENSE COLLABORATIVE

One of CISA's most important roles is serving as a trusted hub for information sharing, but it has recently expanded to include more robust operational and planning collaboration across the public and private sectors. This role was formalized and expanded at the recommendation of the CSC, which emphasized the need for a Joint Cyber Planning Cell "under CISA to coordinate cybersecurity planning and readiness across the federal government and between the public and private sectors."¹²¹ CISA has taken it further by establishing a Joint Cyber Defense Collaborative (JCDC).¹²² In CISA director Jen Easterly's view, JCDC is "more than just planning."¹²³ While the JCDC is still a work in progress, it would be helpful moving forward for there to be more clarity into the changing composition of the group and membership criteria, how it expects to formally coordinate with other information-sharing mechanisms, and what its envisioned role and expected interaction with FCEB agencies are. **While the JCDC has experienced early successes, its ability to provide value in the future will rely on its ability to either scale up or manage a smaller representative group that is trusted as an authoritative coalition by a wide variety of sectors.**

The ultimate goal of the JCDC is to create a common operating picture for federal agencies, industry experts, and critical infrastructure owners and operators so that they can more proactively hunt, plan for, and jointly respond to cyber threats.¹²⁴ Just in the past year, CISA has broadened its focus to include industrial control systems expertise, increasing the diversity and strength of the JCDC's capabilities.¹²⁵ CISA is also collecting information from international sources, collaborating with over 150 partners worldwide to share cybersecurity data.¹²⁶ Additionally, CISA has touted the JCDC's response to the Log4Shell vulnerability and the cyber challenges that arose during Russia's invasion of Ukraine as successes.¹²⁷

Critics of the JCDC point to the office's lack of a formal charter or clear membership criteria, which could potentially hinder future scalability and transparency.¹²⁸ During this project's expert interviews, for example, it was mentioned that the information flow, in all directions, is not happening fast enough.

Relatedly, there are questions about how effectively the JCDC can work in terms of long-term planning (not just during crisis mode) and how it plans to manage its growth in the coming years. Moving forward, it will also be important to see how the JCDC balances ease of reporting and information sharing with more formal concerns about liability. CISA has provided some initial guidance on its website, but there will likely be lingering concerns about liability protection in the absence of more formal assurances. Finally, while there are benefits to using certain commercial

platforms for emergency communications, there will always be concerns about alternatives in case those channels are compromised in any way.

The JCDC will not be effective if *everyone* is a member, but identifying ways to make membership criteria intentional, representative, and relevant will be key, as will be finding ways to demonstrate the value add to FCEB agencies (see Recommendation 3.5 on the value add of the JCDC).

Co-pilots: CISA and Cyber Command's Partnership during a Crisis

During the 2023 RSA Conference, CISA executive assistant director for cybersecurity Eric Goldstein and Major General William Hartman, commander of the Cyber National Mission Force (CNMF), took the stage to provide an overview on how both entities ride side by side to defend the federal enterprise. They shared overlapping goals, with Goldstein emphasizing the desire to help increase costs on adversaries and signaling to actors that a “call to one is a call to all” so that partners overseas also take action—not just the United States. Complementing Goldstein’s overview, Hartman described the CNMF command as “foreign facing,” defending the homeland and supporting its allies, while highlighting that “no partner is more important than DHS CISA.” Both spoke to the level of collaboration they execute, working side by side through liaison officers at each other’s locations, from senior leaders down to individual analysts and operators. Hartman further elaborated that the CNMF is focused on two things: (1) what information does CISA have relevant to the DOD’s missions that might allow it to disrupt or prevent an attack on the homeland, and (2) what does the CNMF observe through operations in foreign space that can be shared back to CISA to protect the homeland?

The importance of the CISA-CNMF partnership proved decisive for bidirectional information sharing during some well-known incidents. The first was SolarWinds: within the hour that FireEye alerted the government, CISA and the DOD began to act. CISA rapidly identified nine FCEB agencies that were compromised. This was followed by incident response to understand the breath of intrusions, the payloads, and the artifacts left behind. Next, CISA extracted infected servers and sent data to the CNMF. On the side of the DOD and the CNMF, Major General Hartford stressed that gaining an image of compromised servers from CISA was invaluable. The CNMF used CISA’s server image for modeling to rehearse and exercise hunting skills, and in the span of a few days, the CNMF developed high-end capabilities to hunt the adversaries. At the same time, intelligence indicated that a foreign partner was compromised by the same actor, and the partner requested the assistance of the CNMF. The CNMF team then deployed overseas and almost immediately encountered adversary activity in their hunt-forward operation. The operation was a success and the CNMF collected novel malware from its encounter and moved to share it broadly.

Returning to the public campaign, CISA reviewed the tactics, techniques, and procedures using information that the CNMF brought back to share with the nine compromised FCEB agencies and more broadly. Thanks to this data, CISA then developed an eviction guide to make sure the malicious actors were out of systems. CISA not only worked with the CNMF but also with the NSA, Mandiant, and Microsoft, forming a united front across the .gov, .mil, and .com ecosystems to kick out the invaders. A united front across the multiple sectors helped lend confidence and credibility in the eviction guide and eased worries for both industry and FCEB agencies to arrive at an eviction point.

Incident Response

During a number of interviews, experts noted that they had been the recipients of CISA's incident response services or, at the very least, that they could understand why these services were an important part of CISA's broader offerings. From providing general assistance to impacted FCEBs to actively coordinating with law enforcement on the investigative aspect, CISA is well positioned to deliver timely incident response guidance and immediate assistance.

Prompted by Section 6 of EO 14028, CISA published incident response and vulnerability response playbooks for FCEB agencies.¹²⁹ Each playbook walks FCEB agencies through the life cycle of an incident, highlighting activities that can be done both during and pre- and post-crisis to ensure that information is collected and shared in a timely manner and that steps are taken to mitigate the incident's effects. Additionally, CISA offers free incident response training for interested federal employees and contractors.¹³⁰ But where CISA, by way of the DHS, becomes even more helpful is that it can engage in both asset response and threat response activities. Presidential Policy Directive 41 designates the DHS's National Cybersecurity and Communications Center as lead for asset response. Separately, while the Department of Justice (DOJ) leads in threat response via its investigatory authorities, the DHS plays a critical supporting role in that process.¹³¹

Moving forward, CISA might consider more intentionally moving away from guidance that focuses on threats and vulnerabilities and instead look to address consequences more broadly.¹³² To the extent that these incident response trainings and pre-incident guidance documents can actively change how agencies think about recovery (and what, in fact, they need to recover from), that might help agencies in the long run. A good example for why the consequence-based approach should be intentionally considered is the Colonial Pipeline incident. Even though the ransomware attack was on Colonial Pipeline's billing system, they had to shut down their entire operational technology (OT) out of concern that the attack was widespread.¹³³ This suggests that anticipating cascading consequences—and even the public perception of a potential incident—should be more intentionally included in incident plans (see Recommendations 2.4 and 3.7 on revisiting mission-essential functions and promoting resilience, respectively).

As a general note to appropriators, while these services are considered valuable, CISA is woefully under-resourced for its incident response activities. These capabilities are not available to all and rely heavily on surge plans from other agencies and the National Guard if there is a large demand.

Resilience Building

As suggested in a recent CSIS study on federal government resilience, resilience can broadly be defined as “how well an individual, institution, or society can prepare for and respond to shocks to the system and endure, perhaps even thrive, under prolonged periods of stress.”¹³⁴ Short of hardening systems, a number of the other initiatives listed above all contribute to CISA’s ability to help FCEB agencies maintain more secure networks and resilient postures overall. However, this study more narrowly categorizes resilience-building activities as those that help FCEB agencies plan for and start building toward long-term resilience. While resilience-building activities are often surpassed or overlooked in favor of activities that seem to focus on the short term or that yield immediate benefits, these operations are key to helping FCEB entities properly plan for future threats and challenges.

Training and Exercises

The United States has invested vast amounts of taxpayer dollars into hardening, evolving, and improving cybersecurity across federal, SLTT, and private sector systems. In addition to investing in technologies and systems, it is just as important to invest in training and process. Similar to how U.S. schools simulate earthquake, fire, tornado, and active-shooter drills to train students and teachers for what they should do during a crisis, CISA simulates the discovery of and response to cyber incidents so relevant actors are proactively mapping out response plans. CISA’s premier exercise is Cyber Storm, where participating organizations are asked to execute strategic decisionmaking and practice interagency coordination to address an incident scenario.¹³⁵

Cyber Storm is a biannual exercise. The most recent one was held in March 2022 (Version VIII), and the next exercise will likely take place in the spring of 2024. Each exercise grows out of the previous one, in a sense building on institutional knowledge and key insights identified during the previous exercise. This process helps new and old players stay up to date on the current concerns and plan through industry best practices.

The latest exercise had a stated goal of “strengthening cybersecurity preparedness and response capabilities by exercising policies, processes, and procedures for identifying and responding to a multi-sector significant cyber incident impacting critical infrastructure.”¹³⁶ The exercise included representatives from 100 private companies across 10 critical infrastructure sectors, 33 FCEB agencies, 9 states, and 15 countries. After running the exercise, the group identified shortcomings and areas needing greater clarity with regard to government policies. Ultimately, the exercise was successful in that it not only helped the different entities practice how they should collaborate and share information during a crisis (something that is routinely needed during an actual incident), but also demonstrated gaps that the government needs to address for future plans to be more effective.

Cyber Storm by itself is a tremendous project, but CISA also publishes general exercise information and encourages the general practice of hosting similar exercises. Whether as a host, facilitator, or participant, CISA should continue to invest in training FCEB agencies to conduct exercises on their own and promote these exercises as a way for agencies to, among other things, map out resilience and continuity of operational plans.

GENERAL GUIDANCE

In general, interviewed industry and FCEB experts seemed appreciative of CISA's guidance documents (see Recommendation 3.8 on transparency guidance). The question then becomes whether it is CISA's role to aid general guidance with additional support for implementation, or if that is something FCEB agencies should be expected to manage on their own or with the support and guidance of other entities.

CISA's role as a general information resource for FCEB agencies cannot be overstated. In addition to some of the service-specific resources listed above, CISA recently published reference guides such as its *Cloud Security Technical Reference Architecture Guide* and *Zero Trust Maturity Model*—both representing the types of comprehensive guides that FCEB agencies can consult to support their respective agency plans to modernize and enhance security in the coming years.¹³⁷

During one particularly interesting interview, a federal CISO noted that CISA's guidance documents are great but that it would be helpful if they could detail out a few subject matter experts to further assist FCEB agencies. For instance, the interviewee thought it would have been helpful for CISA to additionally assign a ZTA expert to the different FCEB agencies to help them with ZTA migration beyond just producing a document (see Recommendation 2.5 on CISA's role with regard to FCEB ZTA migration).

This suggestion raises a few questions. Does CISA have the capacity to offer this type of service? And if not, is it their job to find a way to do so given their role as the designated lead for federal network security? Put another way, what is the actual scope of CISA's mission with regard to FCEB protection, and what are the implications for other entities that directly or indirectly play some role in securing or supporting the maintenance of federal networks?

POST-INCIDENT REVIEWS

The U.S. Cyber Safety Review Board (CSRB) was established by EO 14028 after the SolarWinds incident, and its goal is to investigate significant cyber incidents and socialize lessons learned in the hopes of fortifying national cybersecurity efforts. While some critics have already been quick to call out the board for lack of efficacy, the board is still relatively new, and it is likely too early to fully assess the program.

The board comprises no more than 20 individuals appointed by the CISA director, and it studies and produces recommendations to the secretary of homeland security by way of the CISA director.¹³⁸ To date, the CSRB has investigated the December 2021 disclosure of the Log4j vulnerability, one of the most serious software vulnerabilities in history, and attacks carried out by the Lapsus\$ hacking group.¹³⁹ DHS secretary Alejandro Mayorkas also recently announced that the CSRB will conduct a

review of cloud service providers and their security practices, with a focus on the recent suspected Chinese intrusion into Microsoft Exchange Online.¹⁴⁰

Critiques of the board include confidentiality issues, institutional factors such as a lack of full-time staff, budgetary constraints, and potential conflicts of interest.¹⁴¹ Additionally, there seems to be a reluctance to investigate incidents that are a few years old and a reticence to place blame on a single entity when warranted.¹⁴²

As described, the CSRB can be a very useful tool and opportunity to generate meaningful recommendations. But as important as it is for the CSRB to move quickly with its investigations, incident selection is just as, if not more, important.

SECURING .GOV DOMAINS

For an agency to successfully execute its mission, it must cultivate a certain level of trust. It must operate with high levels of integrity and transparency. One of the most basic ways that FCEB agencies accomplish this is by having a consistently updated and well-managed public-facing website. For the past few years, CISA has taken on the role of protecting .gov domains—a role that might be underappreciated but is key to bridging trust between the public and FCEB agencies.

For 20 years, the General Services Administration managed the security of U.S. federal government internet domains. In December 2020, Congress passed the DOTGOV Act, which designated CISA as the new agency tasked with safeguarding .gov domains.¹⁴³ The DOTGOV Act further specifies that .gov domain services will carry zero or negligible costs for “any Federal, State, local or territorial government operated or publicly controlled entity.”¹⁴⁴ Agencies interested in registering a new domain must first secure an authorization letter and then submit their request through the online .gov registrar form.¹⁴⁵ As the designated .gov manager, part of CISA’s job is to spearhead the registration of new domains, with final approval coming from the OMB.¹⁴⁶ Separately, if an organization requires migrating services online, CISA is exploring using DHS grants to facilitate the process; this is in the design stages with the Federal Emergency Management Agency.¹⁴⁷

Ultimately, the goal of the DOTGOV Act is to ensure the confidentiality of, integrity of, and access to information on FCEB websites.¹⁴⁸ As was noted in a February 2023 OMB memo, “When .gov domains are used for websites, people have greater confidence that the information on those sites is authoritative and trustworthy.”¹⁴⁹ To ensure a seamless, transparent, and secure registration and management process, CISA has created a five-step new domain registration process and a domain security best practices guide.¹⁵⁰

Recommendations 5 and 6 in the domain security guide are particularly noteworthy. Step 5 is a recommendation to sign up for CISA’s free network and vulnerability scanning service called Cyber Hygiene.¹⁵¹ Cyber Hygiene provides regular reports that can help FCEB agencies secure internet-facing systems from weak configuration and known vulnerabilities. Notably, this program was highlighted as a frequently used service in a number of expert interviews.

Step 6 in the CISA best practices guide is for SLTT organizations to join the Multi-State Information Sharing and Analysis Center. The center is designated by CISA to serve as the cybersecurity

information-sharing center for SLTT governments. Some of the services included with membership are access to 24/7 incident response and digital forensic services, IP monitoring, and cybersecurity tabletop exercises.

CISA Cyber Supports to SLTT Governments, the Private Sector, and SRMAs

The focus of this report is solely the cybersecurity services offered by CISA to FCEB agencies. However, CISA services are also widely offered to the private sector and SLTT governments as well. Beyond identifying best practices and possible common trends or grievances about how services are delivered to these different entities, it is important to acknowledge how the current system of distributed security management could ultimately impact an FCEB agency's network security or its ability to fulfill its larger mission.

Ultimately, even though an FCEB agency might seem “cyber secure,” there are lower-level entities that are resource-strapped but provide or deliver critical services in support of an FCEB agency's larger mission. Cyber issues need to be prioritized by department and agency leads; attacks on smaller, vulnerable, critical nodes, even if they are not directly supervised by an FCEB agency, can still impact people's perceptions of the larger organization.

A separate but related relationship that is not fully explored in this report is the one CISA has with Sector Risk Management Agencies (SRMAs). As one industry expert noted, the value of an SRMA is to “translate the good cyber advice into language and protocols that can be understood by [critical infrastructure] operators.” Per this expert, who represents a large entity in a critical industry, CISA has the depth of talent but needs to do more to reach out to stakeholders and encourage partnerships and solicit donations to plus up capabilities, among other activities. Relatedly, CISA should not spread itself thin—it should just be a clearing house and should rely on SRMAs for more support.

Moving forward, one challenge for CISA will be to not only provide high levels of assistance and general guidance but to also strike the right balance between centralizing cyber risk (which could lead to cost savings, especially for smaller and medium-sized entities) and delegating out some tasks to other entities (such as some of the SRMAs) that might have greater expertise and reach in a given sector (see Recommendations 3.2 and 3.3 on coordination with SRMAs, information sharing and analysis centers, and others).

General Gaps

According to the head of CISA's Cybersecurity Division, Executive Assistant Director Eric Goldstein, FY 2021 legislation and EO 14028 shifted the cybersecurity landscape in two dramatic ways. First, new authorities and technologies allowed CISA to proactively engage in system monitoring and

threat hunt, which has greatly enhanced CISA's visibility into and across FCEB networks. Second, and by extension, CISA is now able to develop deeper relationships with the FCEB agencies that it serves. Whereas in its early years CISA's relationship with departments and agencies was transactional, in Goldstein's opinion there is a growing perception among the FCEB agencies that CISA is a partner that wants to help them achieve their security goals—and, for smaller and medium-sized FCEBs, actively take on the burden of managing more of their cybersecurity.

There is no doubt that in recent years, and especially since 2021, CISA has made great strides across several fronts to improve and expand cyber services to FCEB agencies. In fact, with a number of new initiatives and capabilities set to formally roll out in the coming years, it is hard to fully assess where CISA will be even a year or two from now. That said, in this time of growth there are real and perceived potential gaps in services or service quality that CISA and Congress should monitor and address. Aside from the service-specific issues that are listed in the sections above, there were some general trends identified in the expert interviews and discussions that warrant attention.

CAPABILITIES

At a basic level, interviewed experts were eager to see if CISA capabilities could collect and detect intrusions at machine speed and if they could properly integrate inputs from their different services into single repositories to provide actionable intelligence. **Modernization is not just about creating new technological solutions to address old problems. New tools have to integrate with preexisting tools and services to ensure there are no disruptions or visibility gaps.**

Setting aside CISA's actual capabilities (since they will be rolled out in the coming months and years), it is possible to assess general perceptions about these capabilities—namely, whether interviewees expect that CISA will be fully authorized and technically capable enough in the near future to actually perform activities such as advanced threat hunting and real-time information sharing, and whether it will have stronger, more reliable capabilities relative to other government or industry entities that could offer the same or better services.

Among this project's sample of interviewed experts, there seemed to be mixed levels of confidence in CISA's technical capabilities. Some expressed doubt that CISA would be able to accomplish all of its stated goals in the immediate future, while others felt stronger confidence in other government entities' technical capabilities.

As one interviewee expressed, service providers should aim to have strong capabilities, but it might not always be prudent for them to maintain capabilities that far exceed those of the entities they are protecting or managing—in this case, the FCEB agencies. Instead, it is more important that CISA monitor and encourage FCEB entities to have baseline capabilities across federal networks to better facilitate coordination in detection and response.

Finally, as well put by one of the interviewees, “CISA offers a wide variety of excellent services. But they are just that: individual services.” While there are indications that CISA is actively moving to prioritize service integration so that insights and information collected via different channels

are essentially talking to each other, it is worth flagging that, at present, this is a notable gap (see Recommendation 3.6 on system integration).

RESOURCES

A few of the interviewed experts expressed variations of this sentiment: “It’s great that CISA offers free services. But are they always free?” Some programs require long-term tool maintenance costs over time that might not have been initially understood. Others occasionally place time-intensive burdens on FCEB personnel—an indirect and underappreciated cost. And some, while not initially including a financial burden, might ultimately require financial investments if CISA’s services uncover an issue that an FCEB agency needs to remedy. **It is not just a question of if CISA is properly resourced to continue providing services to the FCEB agencies, but also one of whether the FCEB agencies are properly resourced to take advantage of and implement guidance offered by CISA.**

The first concern stems from a larger question of what centralized cyber funding could look like for the federal government and what that might mean for FCEB agencies that are the recipients of funds. At present, and as was outlined in the CDM section of this report, there are questions about the long-term sustainability of tools, with some FCEB entities having a harder time affording the continued use of cyber tools into the future.

At the CISA level, there is also the question of whether the agency is adequately funded to accomplish its intended mission. Recent fiscal trends indicate an escalating commitment from the federal government toward bolstering cyberspace defense. The DOD’s allocation of \$13.5 billion for cyberspace activities in FY 2024—a significant, 20.5 percent hike from FY 2023—underscores this commitment.¹⁵² While this budget seeks to operationalize the zero trust framework and advance next-generation encryption solutions, it also emphasizes industry cybersecurity through the Cybersecurity Maturity Model Certification program and the expansion of the CNMF teams. The integration of these solutions is pivotal, not just as a defense mechanism but as a proactive measure against ever-evolving cyber threats.

For FY 2024, CISA is requesting \$3.1 billion, a 5 percent increase from its FY 2023 budget. Director Easterly testified that if the budget were to fall to 2022 levels (roughly \$2.6 billion), then it would “put [CISA] back in a pre-SolarWinds world.”¹⁵³ The agency has made great strides in recent years to increase its capabilities, and moving forward it will be interesting to see if CISA’s allocated budget will be fully utilized and what services will be impacted first by any funding shortfalls. It is crucial to delve deeper into these matters to ascertain whether the existing fiscal strategy aligns with evolving cyber defense imperatives (see Pillar 1 Recommendations: Resourcing toward Success).

For Congress, it is also important to note that the CSIS research team conducted a public survey with 1,000 individuals from the general public. A statistically significant number of respondents indicated that they do not think the federal government currently spends enough money on federal cybersecurity. While CISA has received funding boosts in recent years, and funding alone will not necessarily guarantee increased security, there would likely be political support for upping the cyber budgets for CISA and the FCEB agencies.

AUTHORITIES

In a 2022 CSIS study on federal migration to ZTA and endpoint security, interviewees noted general confusion about who was leading strategic coordination of larger federal ZTA efforts. The research team attempted to map out the different federal roles, noting that a clearer division of labor needs to be communicated in order to properly measure progress and hold agencies accountable for different tasks.¹⁵⁴

With regard to federal network security, CISA is the designated lead. However, in support of its larger network defense mission, other entities such as the ONCD, OMB, and NIST play key roles in providing overall coordination and general guidance. **In order to successfully defend federal networks, CISA needs a clearer delineation of what its role does—and does not—entail.**

Chris Inglis, former national cyber director, described his role as the “coach,” with CISA serving as the “quarterback.”¹⁵⁵ And in many ways, this relationship has worked well, with the ONCD sometimes advocating on CISA’s behalf at higher-level meetings where CISA might not currently have a seat at the table. Still, some industry and government experts expressed a need for more clarity in roles and responsibilities at all levels, not just with regard to CISA’s FCEB mission (see Pillar 2 Recommendations: Leveraging and Harmonizing Authorities).

RELATIONSHIP MANAGEMENT: SHARED SERVICES

Separate from its formal authorities in managing FCEB network security, **CISA also has to identify ways to exist and provide value in the larger ecosystem of shared service providers.** In other words, can CISA play nicely with others and elevate, integrate, and coordinate with the other providers already in the field? The DOJ, for example, is officially designated by the OMB as a federal shared service provider.¹⁵⁶ CISA has also indicated that the Department of Health and Human Services and the Department of Transportation are vetted shared federal service providers.¹⁵⁷

In addition to deconflicting current service offerings, CISA needs to be mindful of newer entities that can offer complementary services to FCEB agencies. For example, the NSA’s Cyber Collaboration Center, one of the DOD’s officially designated service providers that specifically provides tailored services to entities in the defense industrial base, routinely consults with other DOD providers to ensure maximum coordination and no duplication of services. From CSIS’s research, it appears as though the level of coordination between CISA and non-FCEB protecting entities, such as DOD service providers, may not be as high as it could be. Fairly or not, CISA is now the central point for a number of managed services to FCEB agencies, and the burden falls on them to ensure they are in sync and sharing best practices and resources from other providers across industry and governments (see Recommendation 3.4 on coordinating with other shared service providers).

RELATIONSHIP MANAGEMENT WITH FCEB AGENCIES

CISA is taking active steps to position itself as a “partner” to FCEB agencies, but that also means that it needs to be cognizant of unique FCEB missions when providing guidance and developing plans. **CISA needs to be able to balance security concerns with FCEB agencies’ mandates to perform the tasks that are statutorily required of them.**

One concern identified by interviewees for this report is that an FCEB agency could use certain tools to prioritize security that would hurt or impact the entity's mission in other ways. This issue is all the more important if the ease of use for some technologies or processes is key to an agency being able to perform essential parts of its mission. In the name of trying to encourage FCEB agencies to acquire "secure" technologies, products are pushed out that do not necessarily work in ways that are of maximum real use to the FCEB agencies. In other words, the emphasis on security sometimes does not properly balance considerations related to basic operations.

A related concern is the larger issue of FCEB agencies managing technology debt and dealing with legacy systems that are either integral to the department or agency or are logistically difficult to phase out. In theory, general guidance should be to either phase out or properly secure legacy systems. In specific instances where that might not be possible, CISA should be willing to work with FCEB agencies to identify alternate ways to secure the networks.

CISA already advertises that its services do not operate with a one-size-fits-all mentality. CISA needs to take that one step further in creatively thinking through how it defines, measures, and communicates its actual security goals (see Recommendation 3.1 on CISA's outreach strategy).

MEASURING PROGRESS AND SUCCESS

It is not entirely fair to say that metrics for measuring progress in federal cybersecurity do not exist. For instance, in accordance with FISMA, CISA and the OMB are able to collect information to help them better assess how FCEB agencies are making progress in their plans to implement processes and technologies that enhance federal cybersecurity. Additionally, CISA has noted benchmarks for measuring the success of a number of their services in their latest strategic plan for 2024 to 2026.¹⁵⁸ **Having clearly defined metrics is essential. In the absence of such metrics, it will not only be difficult for Congress to conduct oversight and appropriate funds to grow certain programs, but it will also be difficult for FCEB agencies to justify spending time and resources to engage with these services. Additionally, metrics that fail to properly capture unique areas of progress between different types of FCEB agencies will also possibly create tensions between CISA and its FCEB clients.**

CISA is also likely able to internally track FCEB progress based on the number of services used, the frequency of use, and reporting times, among other metrics. That said, one FCEB interviewee did make the point that CISA might need to be more discerning in how it measures FCEB progress. For instance, if a third-party contractor is failing to meet certain deadlines and performance goals, blame should be assigned to the contractor and not the FCEB agency. An industry interviewee made a similar point, noting that the "matrix of contractors" makes it difficult to see who or what is actually working, and who or what is falling short. The metrics are not necessarily capturing the people and how they can positively or negatively impact progress.

Finally, another gap is a lack of measures that can help the public and FCEB agencies measure the usefulness of CISA's offered services. Beyond use numbers, what are other formal metrics to rank the success (or failures) of certain products and services? And can these be used to generate more buy-in for CISA services? (See Recommendation 2.6 on metrics and FCEB feedback.)

MISSION AND PURPOSE

At what stage is it CISA's responsibility to ensure not only that it is providing resources to FCEB agencies but that all FCEB agencies are taking full advantage of CISA's offered services? In interviews with government and industry experts, there seemed to be varying opinions on this. Some would argue that CISA is already doing a lot and that it is not its fault if some FCEB agencies are not devoting enough time to familiarizing themselves with CISA services. Others thought the burden should fall on CISA to articulate clearly and comprehensively the nature of its services and ensure that they are being widely used by FCEB agencies. This becomes especially true for small and medium entities that, at present, might not have the time or resources to fully prioritize cybersecurity, let alone understand the various aspects of CISA services.

Beyond the public relations consideration, there is a larger issue underpinning this question: **In order to be the designated lead of FCEB network security, does CISA need to centrally manage cyber risk across the FCEB landscape?** Or should it take a tailored approach, letting some departments and agencies responsibly manage their own cybersecurity while taking on the security burdens of smaller and medium-sized entities?

Per the 2023 National Cyber Strategy, "federal civilian agencies are responsible for managing and securing their own IT and OT systems," and federal cybersecurity plans must balance an agency's "individual authorities and capabilities . . . with the security benefits achieved through a collective approach to defense."¹⁵⁹ While it can be assumed that this language was developed in close consultation with CISA, it does potentially diverge from CISA's future goals of being able to manage the security of entities that are unable to sufficiently do so themselves.

For any of the cyber services to be successful moving forward, there needs to be a clarity of mission and long-term purpose. At present, while CISA might operate internally with a clear understanding, its operations are potentially at odds with how others are perceiving CISA's role, and that could impact its usefulness as it continues to evolve (see Recommendations 2.1 and 2.3 on CISA's role, and FCEB leaders' roles, in managing federal networks).

Future Threats and Challenges on the Horizon

For this report, the CSIS research team studied the current state of CISA services in order to better appreciate and predict how these initiatives might fare against future threats and challenges. Assuming current trends continue, the team's goal was to get a better sense of what CISA's overall network defense posture might look like in the coming years in order to identify possible service gaps and necessary interventions that should be considered in the near future.

The research team intentionally limited its scope of study to look at a time frame three to five years out. Instead of hypothesizing major incidents that could arise in the distant future, the research team asked experts and tabletop exercise participants to critically think about realistic threats on the horizon and predict how CISA's maturing services might be able to address these scenarios.

There were some specific mentions of actual technologies adversaries could use that might evolve in the coming years and test the effectiveness of CISA services. However, the majority of comments seemed to emphasize that future threats and challenges to FCEB networks will come from the same or similar threat vectors as seen today, just at greater frequency and likely in combination with other attacks. The challenge for CISA and the U.S. government writ large is finding ways to prioritize and appropriately respond to these types of attacks over a sustained period of time. Additionally, if left unaddressed, ongoing coordination, communication, and resourcing challenges will hamper the collective abilities of CISA and FCEB agencies to effectively defend federal networks.

Reflections from Expert Interviews

Between this research project and a related effort looking at federal cybersecurity budgets, CSIS researchers and affiliates conducted over 30 informational interviews to better understand threats and challenges to federal networks, as well as the state of CISA cybersecurity services offered to FCEB agencies. The following is an overview of the types of individuals that participated in the expert interviews (not including comments from the expert task force and other experts that shared perspectives during the tabletop exercises):

- Seven FCEB CISOs and CIOs
- Twelve federal cybersecurity experts (including individuals representing shared service providers, the ONCD, and CISA)
- Eleven private sector CISOs, CIOs, and cybersecurity experts

These not-for-attribution interviews covered a range of topics, such as personal experiences with and perceptions of CISA's current tools and services, resource allocation, formal and implied authorities, marketing strategies, and future threats and challenges.

Ultimately, even though the interviewed experts represented different-sized public and private sector entities, the CSIS research team was able to capture some interesting trends and notable divergence points between the groups. While specific comments from the interviews helped inform the research team's general research and are reflected throughout the report, this section summarizes some key trends observed across the different interviews.

HOW TO SPEND FUNDS

Invest in data and service integration for greater visibility. Across interviews, the most requested investment was for CISA to prioritize data integration between its different tools and services, especially with regard to information collected via CDM. The desired outcome is to optimize visibility for all FCEB agencies by mapping services back to systems and within risk management tools. Some interviewees also suggested the use of AI/ML to assist with data integration. The observed comments underscore that CISA should prioritize investing in and actually communicating updates on data integration and the use of AI/ML to support greater automation.

Advocate for cyber investments on behalf of FCEB agencies. FCEB interviewees pointed out that there is a role for CISA (or other cyber departments and entities in the federal government) to help FCEB agencies make informed decisions about how to invest in new technologies. A big part of that is helping the CISOs, CIOs, and cyber experts make the case for why their departments and agencies need more cyber investments to enhance security.

Some interviewees, for example, expressed the desire for CISA representatives to advocate on behalf of the FCEB agencies for the use of AI technologies in network defense or to invest in training programs that help FCEB agencies more easily adopt and incorporate future technologies. Another common observation was that CISA can use its platform to help FCEB entities justify and allocate funds for more and better cyber talent. Per one FCEB interviewee, the federal enterprise currently

lacks an advocate on behalf of the FCEB agencies who could resource departments with the proper funding and workforce to manage network security.

Develop sustainable cybersecurity budgets. An important common theme observed across a number of interviews is that FCEB agencies, at varying levels, need support in securing and maintaining cybersecurity budgets over long periods of time. This was most commonly referenced in relation to the CDM program, where FCEB agencies were given subsidies to cover their tools for an initial two years but were then expected to fund the tools on their own once the initial funding expired (see CDM section of the report).

These budgets also need to account for inflation-related price increases, added labor costs for managing certain tools overtime, and unanticipated costs associated with patching and fixing certain tools periodically or as vulnerabilities are discovered.

While CISA's role might not necessarily be to help FCEB agencies strategize their cyber budgets, and there were different thoughts on what type of funding model or models would be most appropriate for different types of tools and services, the larger point was that the current structure is not optimal for producing long-term security benefits (see Pillar 1 Recommendations: Resourcing toward Success).

AUTHORITIES: BALANCING THE BURDENS OF RISK AND ACCOUNTABILITY

Arguably, the biggest discussion around authorities ultimately got back to **who should be in charge of managing FCEB cyber risk and how that potentially impacts resourcing, information dissemination, general accountability, and related concerns.** One interviewee described CISA's FCEB mission as a challenge because the agency had to "work in a kitchen with too many cooks." One extreme that was brought up was the idea for CISA to centralize management of FCEB IT infrastructure, backed with the funding and other resources to fully execute that mission. Pursuing this route would minimize the "cooks" to just one and centralize risk management at CISA. The alternative, alluded to by a number of experts, is for CISA to continue working as a partner in collaboration with FCEB agencies. Beyond general support via its official services, some interviewees expressed a desire to have CISA subject matter experts detailed to their respective FCEB agencies to assist with issues such as overcoming technical knowledge gaps and helping with ZTA migration.

There are major cultural barriers to CISA becoming the sole manager of risk. And even if it could work through those issues with the FCEB agencies, it is not apparent that CISA currently has the ability to serve in this role in the near future. That said, this is a question that should be studied further, especially since there seem to be different ideas about what balance could yield optimal security outcomes (see Pillar 2 Recommendations: Leveraging and Harmonizing Authorities).

COMMUNICATION AND ENGAGEMENT

While experts did note that CISA has been receptive to their comments and feedback, they still emphasized that for CISA to be successful it needs to prioritize persistent but coordinated engagement with FCEB agencies. This is especially important since interviewees also expressed that

some FCEB agencies might not be fully aware of CISA's complete slate of services offered or of the applications or value add in a sector-specific manner. One participant suggested that in addition to a general outreach campaign, a comprehensive, sector-specific service catalog might be helpful.

Some of the non-FCEB experts emphasized that if CISA wants to ensure that new services are used and its authorities appreciated, it should be “knocking on the FCEBs’ doors,” sometimes multiple times, to explain the different services, authorities, and other aspects of its activities. The emphasis should be on the value these services can bring to a department or agency. One expert also made the point that CISA should systematically interview or survey its FCEB clients to identify specific demands for certain types of tools (if it does not do so already). This particular expert further argued that developing a proof of concept and proving its value through demonstrations and success stories will help secure more buy-in for new products and services (see Pillar 3 Recommendations: Enhancing Communication and Coordination with Key Stakeholders).

THE FUTURE THREAT LANDSCAPE

Malware-as-a-service lowers the cost of entry for adversaries, and it is increasing noise for defenders. Interviewees believe that **AI will further increase this noise, and FCEB agencies and CISA should develop and acquire tools that help automate their defenses and increase their ability to detect vulnerabilities** (see Recommendation 1.4 on AI product pricing strategy). One interviewee attested that they are already finding ChatGPT-elevated malware, highlighting that a response to these types of threats is urgently needed today.

A related point is that it is one thing to identify a threat, but it is another to **fully understand the nature of a threat and, by extension, develop the appropriate countermeasures needed to address the situation**. To tackle emerging threats, some interviewees and experts indicated that certain dangers, such as deepfakes, might not immediately appear to pose a threat to federal network security, but that reputational risks and attacks on individuals that manage key parts of an FCEB agency could have detrimental effects on its ability to carry out its mission. A common theme for the interviews was the need to get a better handle on today's threats that could manifest with greater frequency as tomorrow's problems.

Reflections from Tabletop Exercises and the Public Survey

In addition to the interviews, CSIS researchers conducted tabletop exercises and an online survey experiment with the general public to capture how experts and the public think about the cyber threat landscape.¹⁶⁰ The research team ran the tabletop exercise six times. In total, over 50 experts—academics and think tank thought leaders, federal and private sector CISOs, and other cybersecurity or national security experts from the federal and private sectors—participated in the exercises. Conducted in a virtual setting, these exercises delved deep into potential threats surrounding the 2024 U.S. elections. With the overarching scenario of adversaries targeting critical public services, from SNAP and farm loans to vital research endeavors, the exercises highlighted the vulnerabilities that could shake the core of U.S. society.

The participants found themselves in the shoes of hackers advising the hypothetical company Veil Vector Technologies (VVT), strategizing cyberattacks on the public services overseen by the FCEB agencies. With a menu of cyberattacks at their disposal—ranging from the individually targeted deepfakes to more institutionally disruptive degrade attacks—participants were exposed to the multifaceted nature of cyber warfare.

Transitioning from offense to defense, in the next phase participants found themselves representing CISA. Tasked with designing countermeasures against the very strategies they had previously developed, they had to delve into CISA's spectrum of services to assess which might alter adversary behavior. This transition served not just as a strategy assessment tool but also as a testament to the complex task of anticipating and countering cyber threats.

Separately, the CSIS research team adapted the expert exercise and developed a simplified online survey that could be pushed to the general public. The survey was conducted online via Prolific, with 1,000 participants, ensuring a demographic representation in line with the U.S. population. This careful juxtaposition between expert-driven decisions and those of the general public brought forth a nuanced understanding of cyber threat perceptions, potentially bridging the gap between theoretical strategies and their real-world implications.

The multifaceted world of cybersecurity is in continuous flux, with threats originating from both state and non-state entities and ranging from traditional attacks to novel strategies such as deepfakes. Harmonizing insights from experts with public perceptions can pave the way for robust strategies, shaping a safer and more informed digital environment for all.

INSIGHTS FROM THE TABLETOP EXERCISES AND PUBLIC SURVEY

- **Participant Profiles:** The majority of expert participants came from the public and private sectors, supplemented by individuals from academia and think tanks. The public survey, on the other hand, captured U.S. demographic representation.
- **Attacker Choices:** As advisers to VVT, participants were first asked to select which nation-state would be requiring their services. In the second round of the game, the participants were asked to identify what type of non-state actor would require their services. In assessing global threats, experts and the public displayed a divergence in views—especially concerning Russia and China—with the former potentially relying on specialized intelligence and the latter influenced largely by media narratives. This divide extends to perceptions of North Korea, suggesting an information gap where public concerns might be media driven or anchored in broader geopolitical narratives. However, there is a notable alignment in perspectives on non-state threats, possibly due to uniform media portrayals or the transparent nature of such risks. The escalating public concern surrounding “lone wolf” actors underscores the growing recognition of their unpredictability in the digital age.

Table 1: Attacker Choices

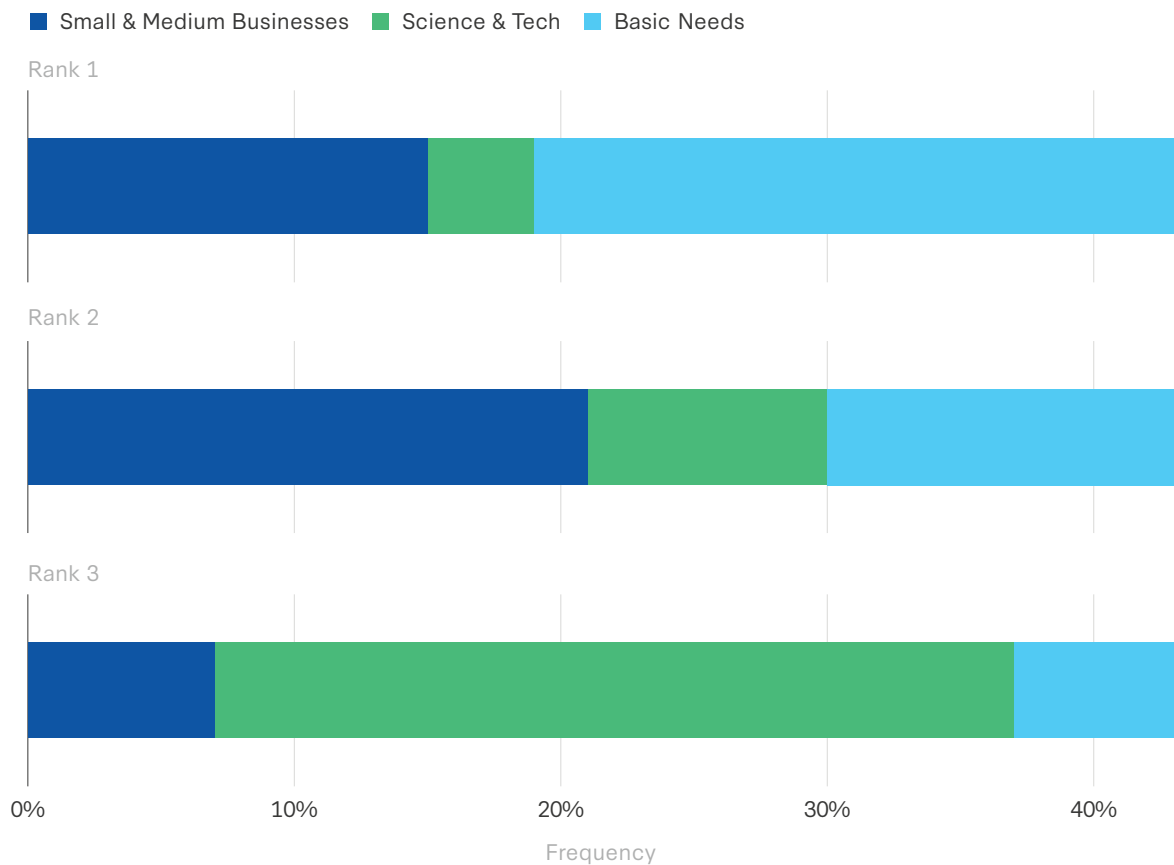
Grouping	Entity	Experts Distribution	Public Distribution
State	China	37%	47%
	North Korea	0%	10%
	Russia	57%	41%
	Iran	6%	2%
Non-state	Alt-Right Group	42%	38%
	Alt-Left Group	10%	9%
	Financially Motivated	46%	44%
	Lone Wolf	2%	10%

Participants were given three options of domains to target in the exercise:

- **Basic Needs:** The deliberate targeting of critical societal elements—such as healthcare, financial systems, and government benefits—can lead to significant chaos. The ripple effect of an attack on these systems could cripple the daily lives of citizens, leading to public unrest, economic instability, and a significant downturn in public trust in institutions.
- **Small and Medium Businesses:** Often overlooked in the grand scheme of cybersecurity, small and medium businesses (SMBs) represent a soft target for adversaries. Due to frequently limited resources, their cybersecurity infrastructure may not be as fortified as larger entities. Their disruption could not only threaten the livelihoods of many but also create supply chain disturbances, causing economic strain and public mistrust toward market institutions.
- **Science and Technology:** Beyond just data breaches, the compromise of the science and technology sector could erode the foundation of factual, evidence-based decisionmaking in society. Misinformation or manipulated data could skew public opinion, lead to ill-informed policies, and erode trust in research institutions, thereby influencing democratic processes in subtle yet profound ways.

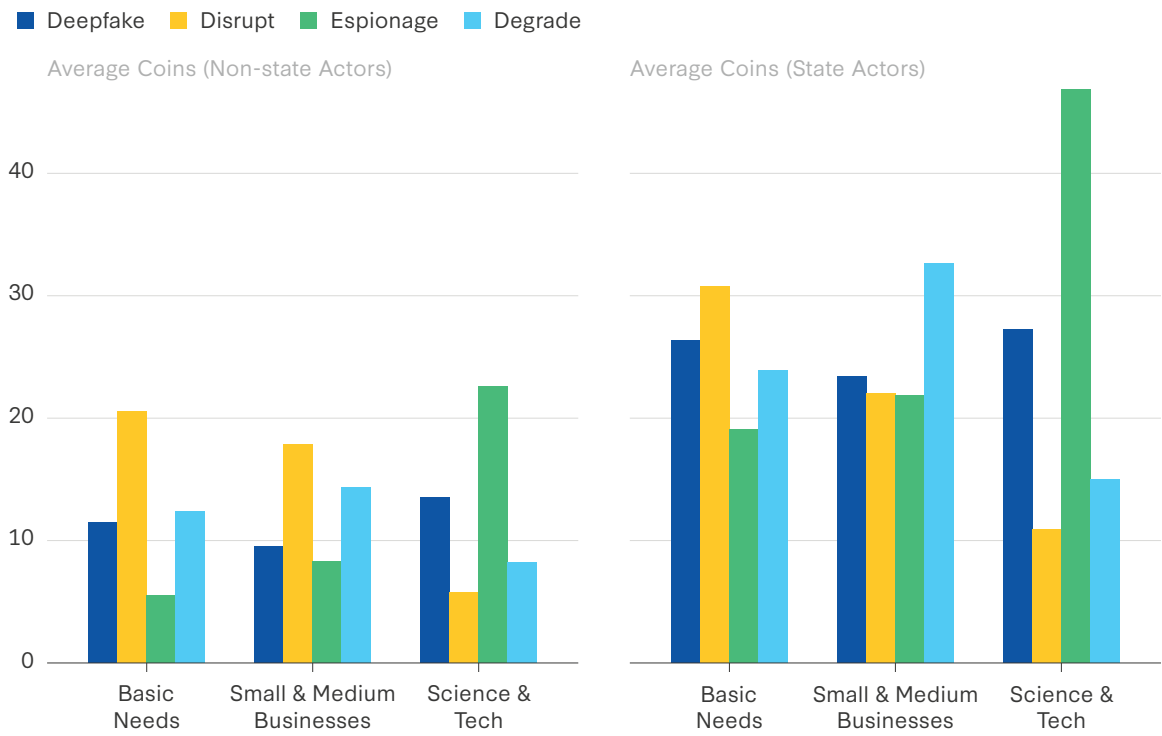
Participants prioritized going after basic needs over SMBs or science and technology. After selecting an attacker, participants were asked what types of services they were most interested in attacking (i.e., which services would most successfully undermine trust in U.S. institutions if attacked). For instance, participants who chose non-state actors gravitated toward attacks on basic needs (52 percent) over SMBs (37 percent), with science and technology being the least preferred target, at 10 percent (see Figure 5).

Figure 5: Distribution of Service Types by Rank (Non-state)



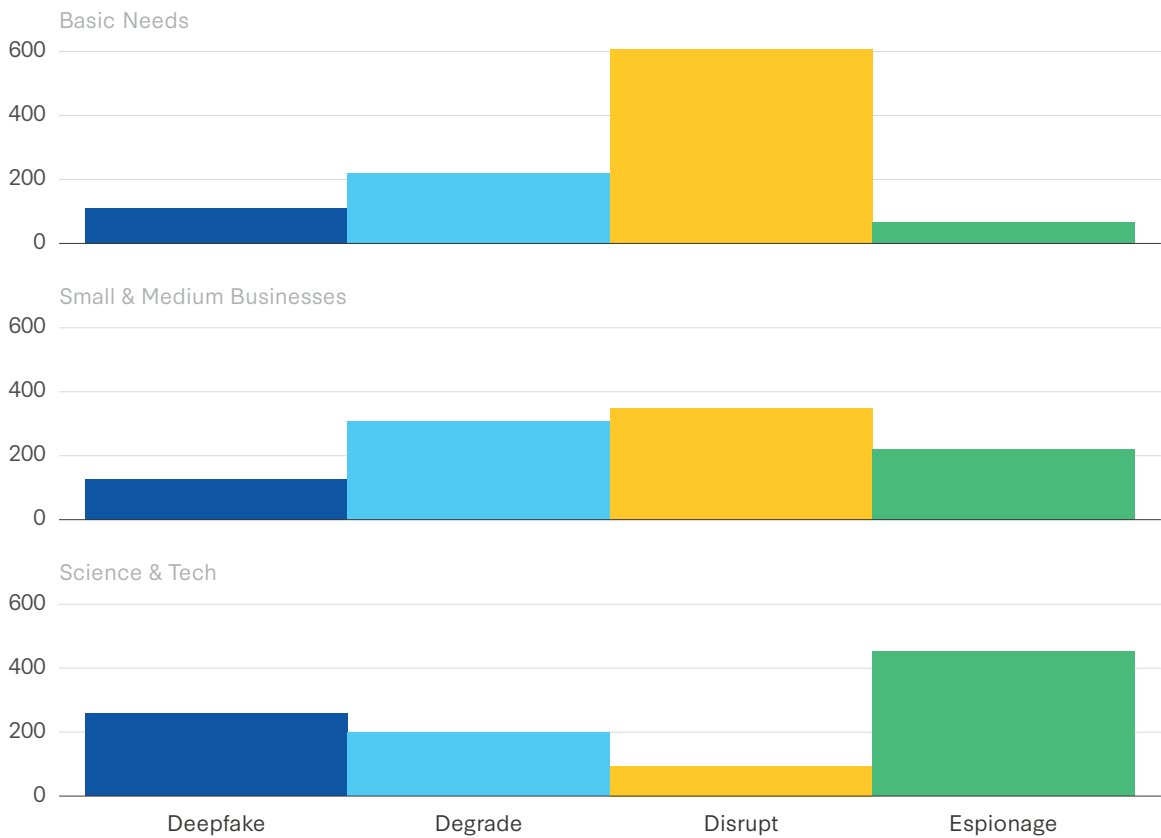
Attack strategies varied depending on what type of service was being attacked. For instance, whether hacktivist or state-sponsored, there was consistency in strategies—basic needs and SMBs were targeted with “Disruption,” while science and technology was susceptible to “Espionage” (see Figure 6). Similar results were obtained from the public survey game (see Figure 7).

Figure 6: Expert Group Average Resource Distribution in Attack Types (Non-state Actors, State Actors)



Note: Due to the simplification of the game for the public audience, the public did not allocate resources to the attack types. Instead, they chose their primary attacks.

Figure 7: Public: Distribution of Attack Types



Attack timing varied depending on if the actor was a state or non-state actor. When players chose state actors, 63 percent opted for a cyberattack strategy focused on future attacks, while 37 percent aimed for immediate results. In contrast, selecting non-state actors saw 56 percent of players planning for future attacks and 44 percent pursuing immediate outcomes. This underscores state actors’ heightened preference for longer-term cyber strategies compared to non-state actors. Additionally, public survey results closely aligned with this expert approach, yielding similar conclusions (see Table 2). There is a statistically significant difference in the attack strategy choices between state and non-state actors, determined by a chi-square test of independence.¹⁶¹

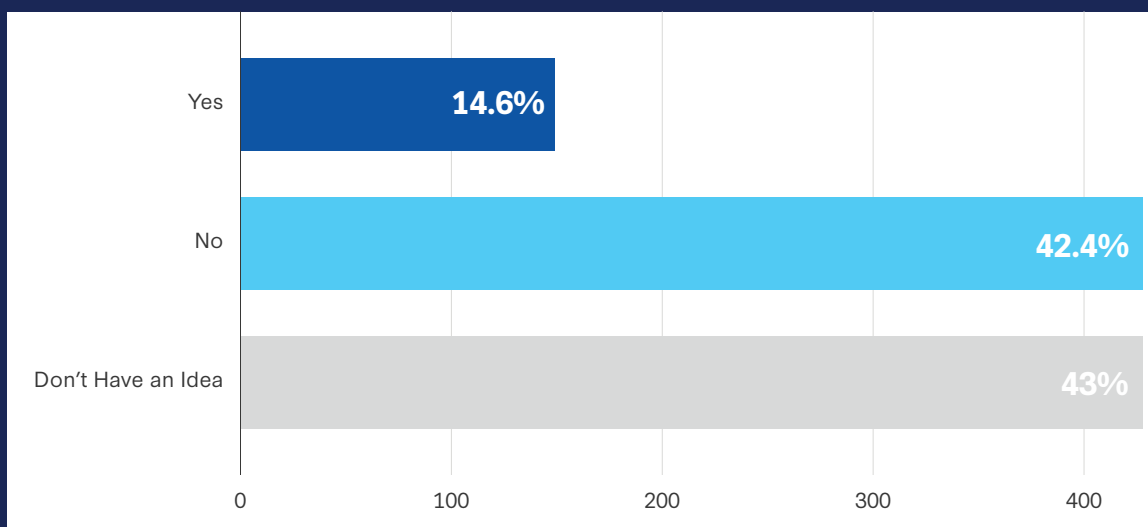
Table 2: Comparison of Attack Strategy Choices between State and Non-state Actors (Public Survey)

Actor Type	Future Attack Count	Immediate Attack Count
State	292	217
Non-state	220	276

Public Perception of U.S. Cybersecurity Spending

The general public believes the federal government does not spend enough on cybersecurity. The public's perception of governmental inadequacy in cybersecurity funding is significant. It implies a gap in public communication—where either the federal initiatives are not well publicized or their efforts are not resonating effectively with the general populace—or just a reminder that there is simply not enough money allocated for cybersecurity. This sentiment underscores the need for improved public relations efforts, clearer communication of cybersecurity endeavors, and potential reevaluation of budget allocations based on emerging threats.

Figure 8: U.S. Funding Survey for Cybersecurity Spending



EMERGING THEMES FROM TABLETOP EXERCISE DISCUSSIONS

In light of the recent tabletop exercise discussions, several themes emerged regarding potential cyber threats targeting federal networks. These insights, gathered from expert deliberations, point to the evolving nature of the cyber landscape and the increasing sophistication of threat actors:

- **Sophisticated State-Sponsored Attacks:** Experts believe that state-sponsored attacks, particularly from adversaries such as Russia and China, are growing in complexity. Their focus seems to be on espionage and long-term presence within federal networks to gather intelligence and potentially influence policies.
- **Deepfakes and Misinformation:** A significant concern raised is the potential use of deepfakes to spread misinformation. Such tactics could be employed to undermine trust in federal communications or to spread false narratives that serve the interests of external actors.
- **Supply Chain Vulnerabilities:** There is increasing awareness of vulnerabilities within the supply chains that serve federal networks. By compromising a single entity within the

supply chain, threat actors can potentially gain access to a broader range of federal systems and data.

- **Erosion of Trust:** One strategy identified involves eroding public trust in federal institutions. By creating disruptions or manipulating data, threat actors can shake the public's confidence in government efficiency and reliability.

Additionally, several themes emerged on how cybersecurity architecture can offset these future threats:

- **Enhanced Monitoring and Threat Intelligence:** Experts suggest that federal networks should invest in real-time monitoring and threat intelligence capabilities. By understanding the evolving threat landscape, federal entities can be better prepared to detect and respond to intrusions.
- **Robust Incident Response Protocols:** In the event of a breach or cyber incident, having a well-defined and practiced response protocol can significantly reduce the potential damage. Rapid containment and mitigation should be the priority.
- **Supply Chain Security:** Given the vulnerabilities in supply chains, experts recommend stricter security standards for all vendors serving federal networks. This includes regular security audits and ensuring that vendors comply with best practices.
- **Public Awareness and Communication:** Experts emphasize the importance of transparent communication with the public. By promptly addressing misinformation and clarifying federal stances, trust can be maintained and the impact of misinformation campaigns can be reduced.
- **Investment in Advanced Technologies:** To keep up with sophisticated threat actors, experts advocate for continued investment in advanced cybersecurity technologies. This includes AI-driven threat detection, encrypted communications, and secure cloud infrastructures.

In conclusion, as the cyber threat landscape continues to evolve, federal networks face increasing challenges. However, by taking a proactive stance, understanding emerging threats, and investing in robust cybersecurity measures, federal entities can effectively safeguard their systems and data. The reflections from the tabletop exercises underscore the importance of continued dialogue, collaboration, and innovation in the realm of federal cybersecurity.

Other Challenges

AI-ENABLED THREATS

Across the board, one of the immediate areas of concern for interviewed experts and tabletop exercise participants was AI-enabled threats and challenges, along with questions about whether the U.S. government's defensive measures would be able to sufficiently detect and address these threats in real time.

Promisingly, statements from CISA leaders demonstrate a perspective on AI that is forward looking, flexible, and practical. Plans were mentioned that not only think about how to help safeguard AI models that might be used for new tools and capabilities but also address how CISA can proactively benefit by using AI tools so it can keep pace with the threat landscape.

The following are a few specific types of AI challenges that could impact FCEB agencies in the coming years, with an assessment of how CISA's planned activities might address these challenges:

- **Synthetic Media and Disinformation:** In recent years there has been growing public awareness about how AI-generated content can be used to spread mis- and disinformation. In a recent CSIS survey, when respondents were presented with a series of images and audio and video clips, they could only correctly identify what content was real versus what content was AI-generated roughly 50 percent of the time, which is basically flipping a coin.¹⁶²

There are attempts by coalitions and individual industry actors to authenticate sources of online content, which is a step in the right direction. From CISA's point of view, it becomes a question of whether it is its role to even be concerned about these types of threats. Whether or not CISA has the capabilities or capacity to deal with mis- and disinformation, let alone AI-generated mis- and disinformation, the core question is: Does its mission to protect FCEB networks even authorize it to engage in this area of work in the first place?

The consulted experts were mixed. Some were unconcerned about AI's actual impact on institutions, while some were very concerned about its direct and even indirect impact on certain aspects of FCEB agencies. Others expressed a concern but were unsure what role, if any, CISA should play in focusing on this threat.

It is the CSIS research team's belief that recent incidents (such as the story involving deepfakes of a DHS appointee in compromising situations) illustrate how these types of attacks might have low impacts to networks but can greatly damage personal reputations in ways that could influence an FCEB's ability to deliver on its mission.¹⁶³ Additionally, manipulated images might impact an FCEB agency's ability to spread timely, reliable information if it is competing with inauthentic and misleading content. While at present CISA does not have a formal role in addressing this type of mis- and disinformation (with the exception of the election context), it might consider exploring some role, especially with regard to cyber-enabled mis-, dis-, and malinformation, since these types of attacks will likely continue in the coming years (see Recommendation 2.8 on CISA's role in addressing mis- and disinformation).

- **Data Poisoning and Infiltration:** Experts were keen to mention that CISA's future successes will rely on its ability to detect and respond to situations at machine speed. Outside researchers should be able to better assess CISA's ability to do this as it rolls out newer capabilities in the coming years. But aside from the capabilities themselves, there are general concerns about the ability of government and industry to safeguard the AI models used to develop these newer tools. An AI-enabled tool is only as effective as the model used to build it, and poisoned AI models could disrupt CISA's ability to respond in certain situations. At an

even more basic level, CISA and other entities ought to look at ways to address unintentional biases and other flawed information that could be used in developing these tools.

A related concern is that adversaries can use AI tools to monitor patterns in CISA's automated threat hunt and detection services and then use that to interfere with, avoid, or generally circumvent capabilities that are in place.

QUANTUM COMPUTING

The threat of quantum computing was not listed as an immediate area of concern, with experts noting that quantum-related threats will likely manifest in five to ten years as opposed to the closer timeframe this study is focusing on. However, CISA should still be prepared to defend against threats stemming from higher computational power.

The most realistic possibility in the near term is adversaries relying on a “harvest now, decrypt later” strategy, whereby exfiltrated encrypted data is stored with the assumption that it can be decrypted by adversaries using post-quantum cryptography algorithms at some later point in time.¹⁶⁴ It is a near-term area of concern only insofar as it further emphasizes the need for departments and agencies to operate with greater levels of resilience—in a way, it is less a matter of if your data will be stolen than when it will be stolen. Beyond any technical solutions, CISA is currently well positioned to provide stronger guidance on how FCEB agencies might concretely anticipate and address these types of situations.

TODAY'S CHALLENGES, TOMORROW'S PROBLEMS

Despite the various possible threat vectors and new technologies that are projected to cause damage in the coming years, the overwhelming majority of experts consulted for this project—regardless of professional background—emphasized that they are most concerned about the ability of the U.S. government and industry to properly manage today's challenges. In other words, the actual cost for adversaries to engage in attacks akin to the ones occurring today will be cheaper in the coming years, and for several reasons they are likely to be waged with greater frequency, which will naturally put a strain on the currently offered support services.

- **Geopolitical Challenges:** At the macro level, festering geopolitical tensions will increase the likelihood that foreign adversaries invest in and deploy cyberattacks that directly target U.S. government institutions. In July 2023, it was reported that suspected Chinese malware was detected across a number of military systems.¹⁶⁵ While China is typically known for its espionage activities, this particular incident is concerning because it looks like the malware could be used to actively disrupt—as opposed to simply surveil—compromised systems.

This departure in China's modus operandi is a general reminder that the threat landscape is changing, and it goes without saying that the strained relationships between the United States and known adversaries needs to be constantly reevaluated in risk assessments. At the operational level, this requires CISA and other entities tasked with a defensive cyber mission to map out all the ways in which these larger issues might manifest into seemingly low-level attacks.

Stemming from this are supply chain risks and vulnerabilities, as well as the question of what explicit role, if any, CISA should take in managing these risks as related to the protection of federal networks.

- **Structural Challenges:** Following the release of the 2020 CSC report, the commission’s cochair, Senator Angus King, repeatedly justified the recommendation for a national cyber director by saying it would give the government “one throat to choke” after a major incident.¹⁶⁶ But it is now a few years in, and cyber authorities—and by extension the accountability mechanisms—are still dispersed. At one level, it is assumed that some variation of today’s issues around general coordination and role delineation might continue to plague the U.S. government in the coming years. Regarding CISA in particular and its role as the lead for network defense, there are promising signs that it has been establishing strong relationships with U.S. government partners and FCEB and non-FCEB entities alike. But it will be essential that CISA continues to push for more role clarity that can translate into greater overall clarity in reporting structures and ultimate responses, especially considering predicted future threat scenarios.

What will be even more interesting in the near future is to see how CISA’s new initiatives actively manage the cyber risk of FCEB agencies, especially small and medium-sized ones. Paraphrasing the remarks of one FCEB interviewee, “all agencies think they are unique snowflakes, but at the end of the day, a hyper-tailored approach can only go so far, and there are certain consistent practices CISA can and must insist on.” With that being the case, it will be interesting to see how much of the security burden CISA takes on from FCEB agencies, how that compares between different agencies, and what the difference is between what CISA actually manages and what it aspires to manage.

Understanding this balance will be particularly important in light of many FCEB agencies transitioning and modernizing technologies in the name of enhancing cybersecurity. CISA will need to be particularly attuned to how efforts to rapidly meet certain U.S. government implementation deadlines might unintentionally create visibility gaps or introduce new vulnerabilities into FCEB systems. The challenge for CISA will be in how it decides to allow agencies to maintain independence in managing aspects such as technology debt from legacy systems, an issue that will be more pronounced in the coming years, while confidently executing its mission as the lead for federal network defense.

- **Workforce Challenges:** In recent years, cyber workforce challenges have been closely examined and well documented.¹⁶⁷ The private and public sectors alike have made plans to address staffing shortfalls. Notably, the ONCD recently published its National Cyber Workforce and Education Strategy, which specifically outlines recommendations and opportunities for the federal government to attract and retain cyber talent more intentionally.¹⁶⁸

As a next step, the government needs to execute these proposed strategies and quickly fill vacancies. This is important not only for actual cyber entities such as CISA but across FCEB

agencies as well. Especially if there is concern that future threats will be more persistent in nature, system resilience will rely on having a sustainable workforce that can also surge in capacity during a prolonged incident. As was observed by one of the interviewed industry leaders, “[the success of CISA services] is less about the CISA programs and more about people.” In other words, success depends on whether the FCEB agencies are well staffed with skilled experts that can take on these different challenges and whether they are coming in with a mindset conducive to working with CISA as a true partner.

- **Societal Challenges:** During one of the convened tabletop exercises, an expert made the following point: the exercise assumes an adversary can effectively undermine trust in U.S. institutions, implying as a premise that people have trust in institutions in the first place.

The polls are clear—Americans have been losing trust in democratic institutions for some time.¹⁶⁹ Mis- and disinformation from foreign and domestic voices alike further exacerbate the situation by selectively promoting information that seemingly resonates with individuals’ legitimate grievances about these institutions. At present, the U.S. public generally does not have the societal resilience to deal with these threats.

Moreover, the United States is a deeply polarized society, and today’s political climate makes it challenging for individuals and organizations to meaningfully discuss issues related to curbing mis-, dis-, and malinformation. The current state of affairs has arguably also chilled federal government entities, such as CISA, from exploring ways to meaningfully identify opportunities to address these threats. These societal vulnerabilities only increase concerns of attacks originating from insider threats, an ongoing issue that some of the consulted experts believe could be an even bigger problem in the next few years.

Recommendations

The federal government stands at a cybersecurity crossroads. In the coming years, CISA will greatly expand its offerings as the lead agency for non-defense and intelligence federal network security. At the same time, the scale, frequency, and intensity of cyberattacks against FCEB agencies are increasing. Both state and non-state actors see opportunities for holding the United States hostage through cyberspace. As a result, money is not enough to solve the problem. The United States needs to imagine new ways of coordinating proactive cyber defense and deterrence aligned with its emerging resources (i.e., means) that promote a change in how to think about network security and resilience.

While it is premature to comment on some of CISA's more recent technical capabilities (or soon to be released capabilities) for individual services, or its proposed backend analytic capability, this study highlights actions that Congress, FCEB agencies, and CISA can and must do to streamline and clarify roles and responsibilities, manage perceptions, and establish clear communication channels in order to ensure that all stakeholders are best positioned to protect federal networks. Congress needs to be prepared to not only further define and scope CISA's role in this space but also to provide appropriate oversight into new tools and capabilities that will be rapidly deployed to meet future threats and challenges. Setting aside service-specific recommendations, CISA will significantly benefit by connecting its services more clearly and directly to the needs of FCEB agencies. By showing the value it brings to FCEB agencies, at an affordable price point, CISA can deliver as a true partner in network security efforts. At the same time, FCEB agencies, while not monolithic, need to operate with a greater understanding of CISA's role in defending federal networks today in order to align the role to their respective individual FCEB initiatives. This requires

adequate funding to enable choices based on merit rather than cost. The national security of the United States requires a CISA that is not bound to the lowest bid.

Pillar 1: Resourcing toward Success

Recommendation 1.1 (for Congress): Ensure consistent, coherent, and flexible funding streams for programs such as CDM.

Currently, the CDM program is structured as a centralized funding model, but only for a two-year period. On the one hand, there would be some benefits to Congress signaling an ongoing centralized funding approach to help ensure greater buy-in and continued use of the CDM program. In the current structure, FCEB agencies are prone to face budget constraints and might struggle when their CDM funding expires. This often leads to a piecemeal approach to tool selection and adoption, with agencies making independent decisions based on their individual budget limitations. This can potentially lead to operational disruptions, incomplete coverage, and inconsistent security postures across different agencies. Moreover, there is a case to be made that programs such as CDM provide a national security function on par with some defense-related programs, and as such, they require multiyear funding enabling enterprise agreements that reduce costs and lock in pricing. While this derails some vendor incentives and high margins, it helps democratize cybersecurity excellence.

However, the reason Congress typically does not grant multiyear funding is because that allows it to provide oversight and make adjustments if certain allocations are not being properly spent. Additionally, if a funding cycle is too long, it could result in the calcification of certain tools and halt innovation. Multiyear funding can help reduce the influence of industry vendors aggressively trying to sell alternative products to FCEB agencies, but it can also unintentionally have the adverse effect of making FCEB agencies too complacent with tools that are already in use.

Ultimately, there are two goals: (1) to provide a more predictable landscape for FCEB agencies participating in the CDM program; and (2) to ensure there is sufficient funding to cover the inventory and security of devices as they evolve. A combination of a working capital funds system, or some flexibility for FCEB agencies to carry over unused funds from previous fiscal year appropriations, might ultimately help provide more consistent funding than what is currently afforded. If nothing else, it will help agencies align their budget requests relative to their cybersecurity risk assessments.

Recommendation 1.2 (for Congress): Fund and formalize a Joint Collaborative Environment.

Congress can help catalyze the cybersecurity common operating landscape. As of July 2023, Congress has yet to authorize a JCE. However, recognizing the need for a “set of highways” that can move information easily between the public and private sectors, CISA has indicated that it will commence work with relevant agencies to start building the infrastructure for it.¹⁷⁰ Congress should formally establish the JCE by law and then appropriate funds within the FCEB structure—and for the JCE specifically—so that CISA’s efforts can be scaled quickly and progress can be tracked and measured.

This type of infrastructure is especially important given the numerous streams of both formal and informal communications stemming from different reporting requirements, and it is imperative that

these streams to and from the public and private sectors are brought together in a meaningful way and are analyzed coherently, benefiting from shared insights rather than just shared information.

Recommendation 1.3 (for Congress): Fund an entity to collect, analyze, share, and adequately protect information about cyber statistics.

CISA should be resourced to host—or assign a third party to host—an anonymized, publicly accessible repository of known incidents and vulnerabilities. The data should be hosted as an application program interface and presented on a public-facing dashboard so that CISA and other outside researchers can analyze the history of cyber incidents while also making projections based on past distributions. Preferably, this dashboard would include information from the public and private sectors so that researchers can have a full picture of the threat landscape. This entity would ideally be housed within and supported by the infrastructure of a larger JCE (see Recommendation 1.2 on funding a JCE).

CISA should ensure that it supports agency-level analysis of pooled data alongside reporting at machine speed. CISA should help agencies understand how to tailor their dashboard so that they can better assess risk at the agency level. This could include collaborative planning teams that deploy from CISA to support the agencies most in need. It should also include building in capabilities to increase the speed of analysis and sharing best practices across agencies.

Recommendation 1.4 (for CISA, the ONCD, the OMB, and Congress): Develop a strategy that locks in baseline prices for computing and storage resources for analytics, AI products, and related processing sold to FCEB agencies.

All signs indicate that CISA is exploring how it can use AI technologies, and engage AI companies of all sizes, to advance its mission. As a part of its AI strategy plans, the study team recommends that CISA include three important areas: (1) routine assessments that test the agency’s readiness to deal with AI threats, (2) talent development and upskilling of existing staff to manage AI systems effectively, and (3) coordination with other departments and agencies that are actively thinking of how to work with AI tools and address AI threats (e.g., the DOD’s generative AI and large language models task force, Task Force Lima).¹⁷¹

But in addition to general plans about how CISA can deal with future AI threats, CISA, the ONCD, the OMB, and Congress should also be actively thinking about how to lock in certain contracts related to common AI tools that might be sold to FCEB agencies. This is uncharted territory, and in order for FCEBs to start proactively thinking about how these tools might fit into their budget, it would be helpful for relevant entities to put down some price points—or at the very least some general guidance—before market pressures drive up the anticipated prices of these tools.

Pillar 2: Leveraging and Harmonizing Authorities

Recommendation 2.1 (for CISA): Commission an independent report, in coordination with the ONCD, OMB, and NIST, clearly articulating CISA's roles and responsibilities as the lead for federal network defense.

What does it mean to be the leader of federal network defense, and what are the formal roles that the ONCD, OMB (including federal CISOs), and NIST play in support of this mission? To help all entities involved better appreciate CISA's role (and its possible limits), it would be helpful for CISA to clearly articulate its current role and what its role could be in the coming years with regard to its FCEB mission. This report should address the mission relative to existing resources and staffing models and identify any key gaps in CISA's ability to secure the .gov with its current set of authorities and funding.

Beyond analyzing CISA's roles and limitations, CISA leadership should also clearly articulate who holds the burden of risk and accountability. If there are anticipated changes in the coming years—for instance, if CISA is tasked to manage more risk for certain FCEB agencies over others—that too should be explained with a plan for how that transition will take place. The 2023 FISMA reform legislation that is currently working its way through Congress is in part intended to help clarify the roles between these different entities.

There is a larger question here as to whether CISA should eventually move toward a model where it directly manages the entirety of the .gov landscape. There are definitely trade-offs: centralized management would hold CISA accountable for any issues with network security and likely will provide cost savings in the long run, but the counter is that CISA then becomes a central—if not single—point of failure. Further, that model would absolve FCEB leaders of responsibility for their own cyber health, even though they control resources and are responsible for all other aspects of security. Moreover, there are some immediate hurdles in that CISA's current capabilities are nowhere near those required for such an effort. FCEB agencies are likely to resist this dramatic change. CISA should provide a report describing the pros and cons of this kind of approach, along with its preferred balance of responsibility and the types of roles it hopes to fulfill in the coming years.

Recommendation 2.2 (for Congress): Designate CISA as the agency to which U.S. government departments and agencies should report a major cyber incident.

Centralized reporting is an essential part of ensuring that all stakeholders have the necessary intelligence about a given incident. While different departments and agencies might still have roles related to certain aspects of the response (e.g., the FBI will maintain primary investigative authority), CISA can still be mandated as the lead entity to which FCEB agencies should report cyber incidents. A central reporting structure will aid in intelligence gathering and providing actionable information back out to the FCEB agencies, as well as their critical infrastructure partners, to include the NSA Cyber Collaboration Center.

The Cyber Incident Reporting Council recently delivered a report to Congress outlining suggestions to align reporting requirements and proposing model language for private entities.¹⁷² The report highlights an often-overlooked basic principle that starts with defining “reportable cyber

incidents” to establish a consistent definition; this definition should be adopted as a model, which also includes language to be amendable by CISA.¹⁷³ Regarding FCEB reporting, there is merit in establishing a common definition for use across FCEB agencies. The next step is to organize reporting under a single, modular forum that captures sufficient data fields—while being amendable if FCEB agencies do not have the proper legal authorities to share but can still leverage such a forum.¹⁷⁴ This will help reduce duplication in individual FCEB processes for reporting and remove additional resource burdens. It is then on CISA to prioritize and coordinate the dissemination of the incidents across relevant stakeholders.

There is also a need to harmonize federal information sharing and communication back to the private sector. CISA and the FBI need to create a plan to coordinate sharing information back to those who report. If the FBI uses information from CISA and has knowledge of the information originators or victims, the latter groups must be informed. Further, it should be made clear that reported cyber threat information in CIRCIA is shielded from use by other agencies such as the Securities and Exchange Commission, as an investigation by such a body was not a stated purpose in the construction of CIRCIA. Done correctly, this data should be pooled and accessible in a dashboard that allows tailored data analytics across the FCEB space. This capability creates a requirement to ensure CISA has filled key billets in incident response, data analytics, and collaborative planning and risk management.

Recommendation 2.3 (for FCEB agencies): Elevate conversations about cybersecurity and network security to leadership levels within the FCEB agencies.

Culturally, federal and private sector CISOs are asked to manage cybersecurity, while CEOs and FCEB leads are tasked with managing the larger entity and ensuring it is functioning properly and able to conduct mission-essential functions. Too often, leaders view these functions as separate, siloed tasks. However, there is a case to be made that today’s cyber threats challenge a business or an FCEB agency’s ability to carry out its basic functions. As such, one of two things (or preferably both) need to happen: (1) cybersecurity conversations need to be elevated to higher leadership levels within an FCEB agency, and (2) CISOs need to be empowered to better lead and manage cybersecurity as a core function of the organization.¹⁷⁵ It should not just be the case that the CISO is the point person if there is an incident. Accountability needs to reside at higher levels within an FCEB agency, and that starts with elevating the importance of cybersecurity. Just like “enterprise security” has become a core tenet in the private sector—particularly the financial sector—that mindset needs to pervade FCEB agencies as well.

To support this effort, CISA should explore forming collaborative planning teams that support CISOs across the FCEB landscape. These planning teams could help with risk assessments, budget analysis, and how best to communicate cyber risks to agency leadership. Ensuring CISA has a large enough cyber workforce to support collaborative planning teams is a key component of defending the .gov.

Recommendation 2.4 (for CISA and Congress): Identify a more visible and practical role for CISA in FCEB ZTA implementation.

When it comes to federal migration to ZTA, the OMB plays a guiding and assessing role, the National Security Council and the ONCD play coordinating roles, and CISA plays an enabling role. More than anything else, CISA provides general resource materials on issues such as best practices that can be used by FCEB agencies to aid in their migration efforts. But CISA could be tasked and resourced to provide more hands-on assistance with implementation.

Not to overextend CISA, but there is an opportunity for the agency to have some designated experts that can further elaborate on the points outlined in the ZTA guidance. Even if it is not possible to detail ZTA subject matter experts to the FCEB agencies, at a minimum CISA can identify outside contractors and experts that might be able to fill this advisory role. CISA can also work with outside groups to conduct studies on ZTA migration-related IT and OT disruptions and advise FCEB agencies on how to address these issues as they arise.¹⁷⁶ Collaborative planning teams again provide a possible framework, with CISA deploying support to agencies as they manage the ZTA transition.

An even more radical approach would be to fund CISA as a core aspect of their CDM next-generation approach to provide a centralized “Zero Trust Center of Excellence,” with close coordination with NIST and the OMB, to guide FCEB agencies along a zero trust architecture, roadmap, and implementation plan. While centralized, it should be tailored to the priorities and unique aspects of each agency or component. Again, collaborative planning teams—if sufficiently staffed—could play a critical role in supporting CISOs across the FCEB landscape. CISA collaborative planning teams could be deployed to agencies identified as needing assistance and bring with them expert insights on how best to implement new ZTA guidelines. In this line, CISA can establish a shared services environment similar to the Defense Information Systems Agency’s Thunderdome, where agencies that are not well resourced can access integrated capabilities to increase their zero trust maturity. Regardless of the approach, the transition will be complex. There is no master list of all federal systems online at any one time, and each agency will likely have varying rates of adding new systems and even cloud services that complicate implementation. This complexity is why CISA should analyze its current staffing levels and consider building collaborative planning teams.

Recommendation 2.5 (for CISA and Congress): Develop tailored metrics to measure the progress and integration of new tools.

As mentioned earlier in this report, there is a need for more creative metrics to measure actual progress with CISA’s cyber services to FCEB agencies. For CISA, the challenge is to identify internal metrics that can realistically show progress without unintentionally overburdening FCEB agencies, as well as to measure security outcomes more holistically than simple program outputs.

Moving forward, the metrics should focus on not only the progress of individual tools and processes (e.g., the progress of implementing the tools and separately measuring how these tools enhance cybersecurity), but also CISA’s ability to integrate new capabilities with preexisting tools. The more clearly defined the metrics, the easier it will be to hold CISA accountable for what it is uniquely authorized to accomplish.

Moreover, as CISA collects feedback from FCEB agencies, the research team encourages it to formally leave space for narrative responses as to why certain FCEB agencies either have not met a certain goal or are actively not planning to, and how they plan to mitigate the risk in alternative ways. If certain metrics are focused on outcomes, FCEBs should be given room to more fully explain how they are meeting security goals in ways other than what is recommended or otherwise required by CISA.

Recommendation 2.6 (for CISA and Congress): Dedicate after-action reviews to better understand progress and issues related to CDM.

Related to the need for better metrics in general, every interviewee had very specific but varied feedback on the CDM program, highlighting a need for a formal lessons-learned or after-action process and better metrics for measuring progress with CDM. With new project developments set to take place in the coming months and years, CISA (at the request of Congress) should be prepared to (1) highlight challenges with implementation, (2) outline results or the efficacy of CDM once implemented, and (3) propose realistic next steps for CDM as it relates to specific departments or agencies.

Recommendation 2.7 (for CISA): Identify a way to effectively engage in the mis- and disinformation discourse.

For reasons outlined earlier in this study, the federal government has struggled to find a meaningful and appropriate role in addressing mis- and disinformation. Cyber operations can and have been used to further information operations that impact CISA's mission. Elections come to mind as an immediate example, but there is also cyber-enabled disinformation that can lead to the sabotaging of electric and communications facilities, for example, or that undermine trust in public institutions and objective information put out by the federal government. At the same time, the issue can create a perception of government overreach that makes it difficult to create an objective policy debate around a core national security challenge.

While this issue is larger than CISA, the agency has a role. As a first step, it might make sense for CISA, perhaps through the CSRB, to formally study recent incidents of high-profile cyber and cyber-enabled disinformation campaigns. The committee could then come back with a series of recommendations for how CISA and other entities might most appropriately be involved in understanding and addressing the risks that misinformation poses to CISA's mission moving forward. As part of this effort, the CSRB may need subpoena authority.

Additionally, CISA should consider working with outside researchers to develop training exercises and workshops for FCEB employees that teach them about threats related to mobile device management and walk them through plans for addressing these issues. Most important is to ensure that federal agencies understand how mis- and disinformation, especially when enabled by cyber operations, have the potential to undermine the provision of public goods through cyberspace. These efforts will almost certainly include addressing computational propaganda designed to smear individuals and institutions.

Recommendation 2.8 (for CISA): Develop risk strategies that accompany ONCD and OMB financial planning for the FCEB agencies.

In theory, FCEB cyber budgets are coordinated with the ONCD and OMB. But in the longer budget-approval process, essential line-item requests are deprioritized, underfunded, or completely stricken from the final budgets that are ultimately approved by FCEB leadership, the OMB, or Congress. To help federal CISOs and CIOs more effectively advocate for larger cyber budgets, CISA should consider developing risk profiles that accompany the budget plans. In a sense, these risk assessments would highlight what types of risk an FCEB agency might incur if certain tools or services were not adequately funded. Additionally, CISA, in partnership with FCEB entities, could map out how different types of tools might serve an agency's larger security strategy and support its overall mission, as opposed to looking at tools as one-off fixes to address cyber concerns. Not only can these risk profiles be used to help FCEB agencies advocate for necessary funding, but they can also be used by the executive branch to compare different FCEB agencies.

The White House could consider some sort of ranking system whereby the leaders from low-scoring FCEB agencies have to meet periodically with a designated White House leader to explain (1) why their scores are so low, and (2) what plans they have in place to improve their risk score. Whatever method is adopted, it will have to incentivize CISOs from across the FCEB landscape to participate.

Risk profiles should leverage the granular visibility that CDM has into agency enterprise in a way that is both (1) at object level, so that it can be tied to specific agency components and systems, and (2) near real time (i.e., machine speed) where possible. Second, these profiles can be linked together to provide actionable and contextualized risk recommendations at both the policy and algorithm level (i.e., CDM's AWARE risk algorithm). Here again, CISA could deploy collaboration planning teams and experts to help agencies manage risk, including integrating their risk management strategies with tailored dashboards, ZTA implementation plans, and budget submissions.

Pillar 3: Enhancing Communication and Coordination with Key Stakeholders

Recommendation 3.1 (for CISA): Develop a public campaign to promote CISA's role as the lead for federal network defense.

As an agency, CISA has worked hard to establish a recognizable brand, particularly with the private sector. CISA has a very visible social media presence and can be lauded for putting out periodic updates (such as its first two strategic plans) on where it hopes to go in the coming years. However, there is room for CISA to be more coordinated in its marketing, especially with regard to services offered to FCEB agencies.

From cleaning up its website (and deleting outdated content) to creating a more intentional rhythm for periodic updates with an updated service catalog specifically for FCEB agencies, CISA could benefit from simplifying its messaging. This will also be helpful for FCEB agencies to better understand the full suite of current CISA offerings.

Related to this, interviewees noted that some of CISA's programs, such as CDM, could benefit from more positive communications about success stories and upward trending metrics. These stories can paint a picture that the process is working and that FCEB agencies would be well served by participating to the fullest extent possible.

Recommendation 3.2 (for CISA): Establish a framework for more consistent coordination with SRMAs, information sharing and analysis centers, and other activities with regard to FCEB protection.

One of the comments that came up in private sector interviews is that there are networks and entities that already work with CISA in other capacities that can likely be more plugged-in to support CISA's FCEB mission. While this might already be inherently baked into CISA's plans, it might help for CISA to formally map out its existing stakeholders and clearly identify how each can specifically support CISA's FCEB mission.

Recommendation 3.3 (for CISA): Provide sector-specific cybersecurity guidance, especially for low-security sectors with "soft targets."

Gaps in CISA support across the 16 critical sectors and FCEB agencies exist not out of willfulness or lack of direction but due to inherent limitations driven by budget constraints, staff bandwidth, and talent availability. However, it is likely that CISA will continue to acquire, train, and retain talent and grow to meet the expanding cyber picture. What CISA could do in the short term is review the 16 critical infrastructure sectors on a triannual basis to assess and prioritize three to five "soft target" sectors. In this manner, at a minimum CISA will assist these sectors to improve their cyber resilience, conserving staff bandwidth and prioritizing the entities and agencies that need the most help. This tiered approach could help CISA defend the .gov while it grows its capabilities and talent. The approach also lends itself to generating and deploying collaborating planning teams that focus on integrating risk management with budgets and strategy at the agency level.

Recommendation 3.4 (for CISA): Host a database of shared service offerings for FCEB agencies.

CISA's website already advertises cyber services offered by the Departments of Justice, Transportation, and Health and Human Services.¹⁷⁷ It also mentions that there are efforts in progress aimed at vetting other services and providers that will be included on the website at a later date. Whether by CISA or some other entity, it should be a priority that one of the shared service providers manage a public database that clearly outlines which departments and agencies are current providers and what their specific offerings are.

CISA might even consider hosting an annual or biannual consortium of federal shared service providers to discuss best practices, share insights, and discuss current gaps, among other activities. Given CISA's authorities and reach, the agency is in a strong position to host this sort of convening. This forum would also offer an opportunity to introduce agencies to collaborative planning teams or other services that CISA provides to support defending the .gov.

Recommendation 3.5 (for CISA): Explain the value add of the JCDC to FCEB agencies (separate from the value add for the private sector).

The JCDC continues to provide value for public and private entities alike and has already had some early successes.¹⁷⁸ Moving forward, it could be helpful for FCEB agencies writ large to have clearer direction on the value that the JCDC can have for their respective agencies. Moreover, FCEB agencies should be more aware of which organizations comprise the JCDC, along with why and how their individual needs are being addressed by the select FCEB leaders represented in the group.

Recommendation 3.6 (for CISA): Prioritize (and communicate) system integration when rolling out new capabilities and programs.

One of the identified gaps in CISA's services is that, at a minimum, there is an outside perception that CISA's tools and services are distinct lines of effort. It is not clear that information and best practices are being consistently shared between platforms. In many ways, this is a hard issue for CISA to address, especially given that some of the services offered predate CISA and might have previously operated under different parts of the DHS or other agencies altogether. In other words, when developed, some of these services were not intentionally designed to be integrated with other tools and services.

CISA does appear to be actively trying to address this issue, notably by having CADS serve as a data repository that collects information from these various points. However, as CISA continues to make promises on scaling up, modernizing, and generally updating its capabilities, it needs to more intentionally map out and communicate how these lines of effort work within existing programs. The lack of such planning could lead to problems down the road, as well as potential visibility gaps.

Recommendation 3.7 (for all): Operate with a clear understanding of what it means to have resilient networks and processes.

Cybersecurity is an exercise in risk management, not risk elimination. While that might be something that CISA, some of the more cyber mature FCEB agencies, and federal CISOs are aware of, it is not a clearly understood concept across the board. In its larger public awareness campaigns, it is important that CISA not only call out the importance of resilience by name but actually define in practical terms what that means for an FCEB agency with regard to its federal network and processes.

Recommendation 3.8 (for CISA): Explicitly promote transparency as a way of achieving greater resilience.

The ubiquity of data coupled with today's advancements in cyber technology mean that it will be impossible for FCEB agencies, even after implementing all appropriate safeguards, to assume that sensitive information will not be compromised. With that in mind, CISA can use its platform to more intentionally—via guidance documents and planning manuals—tie the value of transparency to greater resilience for FCEB agencies. In other words, it can highlight why operating with transparency can provide greater resilience and result in less reliance on sensitive information.

Beyond that, CISA can promote transparency across a number of other lines of effort: in incident reporting, in opening networks for outside researchers under careful bug bounty programs to find

weaknesses, among the vendor community in coming forward with vulnerabilities in products, and between government and industry with regard to sharing vulnerabilities, among many other efforts.

Transparency, as it relates to cybersecurity, is not something FCEB agencies will necessarily invest in or prioritize, but CISA can lead the way in providing actionable recommendations for how to operate in this type of environment.

Other Ideas

While the task force had broad agreement on the recommendations above, several other ideas emerged over the course of the study that either did not achieve consensus or were beyond the scope of the current effort. Below, the core research team captured the aspects most relevant to generating a larger dialogue about how to secure the .gov.

WORKFORCE

While progress is being made in the cyber workforce, it is not yet clear whether current efforts are sufficient, given enduring challenges associated with the issue.¹⁷⁹ The new National Cyber Workforce and Education Strategy (NCWES) is certainly a step in the right direction that looks at the problem holistically.¹⁸⁰ The strategy acknowledges the need for hiring and pay flexibility, but it is not immediately clear how to create the type of incentive pay required to attract and retain talent, much less who should pay for additional personnel costs. Leaving over 100 federal agencies to pick up the tab risks creating “haves” and “have nots” because of internal budget challenges that accrue as they pay for approved CDM suites alongside expanded pay incentives for a cyber workforce.

There are also significant communication issues associated with ensuring that current and prospective members of the cyber workforce understand which federal benefits they can take advantage of. According to the strategy, “in fiscal year 2019, only 320 IT Specialists out of the more than 84,000 eligible benefited from student loan repayments. As a second example, critical pay authority is currently available for 800 positions, and only 47 have been used (data provided by [the Office of Personnel Management]).”¹⁸¹ In addition, even when agencies grant additional authorizations to increase pay, the implementation can lag. According to the strategy, “the Secretary of Homeland Security and the Attorney General have been granted the authority (by sec. 401 of the Abolish Trafficking Reauthorization Act of 2022, Public L. No. 117-347, 136 Stat. 6199 (2023)) to provide increased incentive pay to DHS and Department of Justice employees identified as possessing cyber skills. As of this writing, these authorities have not yet been implemented.”¹⁸²

Resource challenges are also likely to confront expanding education opportunities. While the NCWES expands the number of universities offering cybersecurity education through NSF and NSA outreach programs, the resources do not match philanthropic efforts. For example, the Craig Newmark Foundation alone will invest more than the NSF, NIST, and Department of Labor on cybersecurity education and training through its \$100 million Cyber Civil Defense Initiative.¹⁸³ It is also not immediately clear how some lead agency efforts contribute to the vision as part of the NCWES. For example, CISA’s contribution to the effort was a Cyber Security Awareness Month

initiative focused largely on media outreach. No amount of media outreach is likely to address the growing shortfall of IT professionals in the cyber workforce.

INFLATION PROOFING

The entire congressional appropriations process struggles with the challenges posed by higher inflation. The same is true with cybersecurity, where vendors increase the costs of software and contractors increase labor costs. Therefore, the U.S. government—and especially Congress—needs to explore mechanisms for making FCEB agencies more resilient to inflation. Currently, only select mandatory entitlement programs are indexed to inflation.¹⁸⁴ Congress should consider studying current dynamics around cyber funding, specifically how in some cases the projected costs for essential security tools and services might make it difficult for some FCEB agencies to consistently use those tools in the future. Congress should also be monitoring unforeseen operations and maintenance costs associated with managing or updating tools or services. While not possible for all tools, Congress should consider if there are unique circumstances or a specific set of services that should be indexed to inflation or what other mechanisms are available to address sudden cost spikes. If Congress does pursue this type of action, it should frequently revisit which tools and services qualify, so as to not unintentionally block the use of other tools that might perform better than those currently in use.

PREPARING FOR AN ALGORITHMIC FUTURE

Beyond pricing, there is a need for a larger set of standards guiding AI model assurance and testing as well as red teaming generative AI models, but this is outside the scope of the current report. The Biden administration is still in the process of developing a larger policy framework that will affect this evolving technology. For example, the Office of Science and Technology Policy has proposed a blueprint for an AI bill of rights.¹⁸⁵ This initiative parallels multiple high-profile efforts, including the 2021 Federal Data Strategy, the 2021 National Security Commission on AI's final report, the 2023 National Artificial Intelligence Research Resources task force report, and NIST's AI Risk Management Framework.¹⁸⁶

With respect to cyber defense, the most important output from these AI initiatives rests in technical standards for testing and evaluation. These standards will need to include red teaming generative AI models to combat misinformation and deepfakes as well as requirements for vendors selling AI-enabled threat hunt capabilities.¹⁸⁷

Last, the standards must include more detailed requirements for cloud security. There is no AI without big data, and there is no big data without cloud computing. Failing to secure the cloud would create a back door into corrupting new AI/ML applications.¹⁸⁸ At the same time, there is optimism that generative AI applications offer opportunities to enhance security.¹⁸⁹

Once broader federal and technical guidelines are established, CISA will likely need to develop an agency-wide AI strategy focused on limiting the ability of threat actors to hold the United States hostage in cyberspace using malware tailored by generate models. Securing the .gov domain space will require AI applications at multiple levels.

USING A JFHQ-DODIN MODEL TO FURTHER CENTRALIZE THE .GOV ECOSYSTEM

A more radical approach to securing the .gov space would be to centralize budgets, authorities, and operational response across the over 100 federal agencies that constitute it. This approach could, in principle, parallel how the DOD created new entities to defend its networks.

During the Obama administration, the DOD sought to better align its cyber capabilities, including protecting defense networks, building on over 10 years of Joint Task Forces and other command and control constructs.¹⁹⁰ As part of this effort, the DOD created the Joint Force Headquarters - Department of Defense Information Network (JFHQ-DODIN) in 2014, based on earlier plans by U.S. Strategic Command.¹⁹¹

The original concept of operations started from the premise that defense networks are contested battlespace that require centralized planning, control, and named operations (e.g., Operation Gladiator Phoenix, Operation Gladiator Shield) to defend the network.¹⁹² According to Admiral Mike Rogers, this construct also meant that JFHQ-DODIN could assume operational control of different cyber mission forces as part of its defense mission.¹⁹³ In other words, the creation of a centralized task force to defend DOD networks was not just about budgets and authorities; it represented a planning and risk management framework.

Applied to CISA, the JFHQ-DODIN model implies a higher degree of centralization. Agencies would see reduced budgets and personnel if functions normally performed by the CISO were centralized and incident reporting, response, and risk management were performed across the network by federated teams under operational control of CISA. In some ways, this centralization is the natural evolution of the .gov top domain management started in 2021.¹⁹⁴

Yet the option is also not a panacea. The DOD still struggles to report and address cyber incidents, including in the defense industrial base.¹⁹⁵ Centralizing budgets and authorities across over 100 federal agencies would take time, cause friction, and, despite increased visibility (i.e., CDM) and responsiveness (i.e., threat hunt), might not create cost savings.

GETTING THIRD-PARTY RISK RIGHT

In the near future, a large number of government services will transition to a cloud-based architecture. CISA's recent guidelines for "security-by-design" and "security-by-default" linked to pillar three of the 2023 National Cyber Strategy offer a start but not an end to the effort to manage risk in the cloud.¹⁹⁶ There will need to be additional studies and experiments to test how best to manage third-party risks during the cloud transition. Even the best defense still leaves holes dedicated attacks could exploit, and the cloud creates opportunities to capture and exploit a larger array of services. In addition, there will need to be renewed efforts to engage on "security-by-design" internationally through forums such as the International Technical Union. In the twenty-first century, standards are strategy. The best way to manage third-party risk will be to build in technical standards that make digital infrastructure harder to compromise.

The Future of Collective Defense

In the next three to five years, CISA's challenge will be not only to grow and integrate its capabilities, but also to clearly communicate its capabilities to partners and adversaries alike to enhance deterrence.

One of the more concerning aspects of the SolarWinds software compromise is not just that the malware comprehensively penetrated over 200 U.S. government and allied systems as early as 2019.¹⁹⁷ It is that it was able to do so at a time when CISA, FedRAMP reporting, CDM and EINSTEIN, and a host of other agencies, capabilities, and processes were in place that should have, in theory, more quickly detected the intrusion.

One of the key takeaways from the expert tabletop exercises is that while knowledge of CISA services encouraged a few of the attackers to change their attack strategy, most of CISA's services, while important to have, did not greatly factor into the attackers' analyses. The experts came to these conclusions from a few different perspectives. Some believed that the benefits of CISA cyber services, such as those that promote system and process resilience, could only be realized in the long term and would not fully be realized in the immediate future, thereby making them ineffective as deterrents. Others were skeptical that CISA's capabilities would be sufficiently advanced in the near future. And some of the experts did not believe that CISA alone with its defensive posture could undermine an attack strategy without reinforcements from other government entities with investigatory or prosecutorial powers.

But the truth is that with increased resourcing, CISA is making meaningful steps to not only up its capabilities but also make sure those capabilities are integrated and provide a greater picture

of the threats and vulnerabilities that FCEB agencies need to address. CISA's current capabilities, combined with planned reporting requirements and processes, will ensure that the agency has a more fulsome global cyber activity picture. CISA is well positioned not only to monitor and collect information but also to disseminate the information and help entities plan their responses at different levels. The challenge is to ensure CISA can adapt to the evolving threat landscape while navigating bureaucratic challenges.

About the Authors

Benjamin Jensen is a senior fellow for future war, gaming, and strategy in the International Security Program at the Center for Strategic and International Studies (CSIS). He is also a professor of strategic studies at the Marine Corps University School of Advanced Warfighting. Dr. Jensen has spent the last decade researching the changing character of political violence, technology, and strategy. He has worked with the Defense Advanced Research Projects Agency (DARPA), Marine Corps Warfighting Lab, NATO, the U.S. Army, and a range of government agencies and foundations to develop wargames and scenario-driven exercises exploring strategy, defense analysis, crisis response, military planning, and complex emergencies. Outside of traditional defense and security issues, he supported the Economic Community of West African States (ECOWAS) in developing a human security assessment framework and a red team manual for early-warning analysts and development practitioners. He is the author of four books including *Information in War: Military Innovation, Battle Networks, and the Future of Artificial Intelligence* (Georgetown University Press, 2022), *Military Strategy in the 21st Century: People, Connectivity, and Competition* (Cambria, 2018), *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford University Press, 2018), and *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford University Press, 2016). Most recently, he served as the senior research director and lead author for the U.S. Cyberspace Solarium Commission. Dr. Jensen is a graduate of the University of Wisconsin-Madison and received his MA and PhD from the American University School of International Service. He is also a reserve officer in the U.S. Army.

Devi Nair is a former associate director and associate fellow with the CSIS Defending Democratic Institutions Project, where her research focused on cyber and disinformation operation efforts aimed at undermining trust in democratic institutions.

Yasir Atalan is a PhD candidate and a graduate fellow at the Center for Data Science at American University. His research focuses on civil-military relations and international security implications of technology. Methodologically, he is interested in Bayesian analysis, machine learning, and large language models. He is a replication analyst at Political Analysis. He holds an MA in Middle Eastern studies from King's College London and a BS in political science and international relations from Bogazici University.

Jose M. Macias is a research associate in the Futures Lab within the International Security Program at CSIS. He is also a Pearson fellow and teaching assistant at the University of Chicago's Harris School of Public Policy. With a keen interest in the quantitative study of war, Jose's research delves into topics like cross-domain conflicts, societal impacts, and the integration of machine learning in international relations research, with prior significant contributions to the Correlates of War Project, including notable work quantifying the effects of U.S. bilateral counterterrorism treaties in the Global South and eastern Europe. He also previously held positions as a cyber strategy intern

at the U.S. Department of Defense and Army Cyber Command, working to expand the Dyadic Cyber Conflict Dataset (v 2.0), and as a fellow with the Congressional Hispanic Caucus Institute (CHCI), serving under U.S. senator Angus S. King. Jose is pursuing his master's in public policy at the University of Chicago's Harris School of Public Policy, with a special focus on data analytics. His academic journey as a first-generation student includes securing an AA in political science from Fullerton College and a dual BA in political science and international relations from the University of California, Davis.

Endnotes

- 1 “Federal Civilian Executive Branch Agencies List: CISA,” Cybersecurity and Infrastructure Security Agency (CISA), n.d., <https://www.cisa.gov/news-events/directives/federal-civilian-executive-branch-agencies-list>.
- 2 Brandon Valeriano and Benjamin Jensen, “Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report,” in *13th International Conference on Cyber Conflict*, ed. T. Jančárková et al. (Tallinn, Estonia: NATO CCDCOE Publications, 2021), https://ccdcoe.org/uploads/2021/05/CyCon_2021_Valeriano_Jensen.pdf; and Mark Montgomery et al., *Cyberspace Solarium Commission Report* (Washington, DC: U.S. Cyberspace Solarium Commission, 2020), <https://www.solarium.gov/report>.
- 3 “Executive Order on Improving the Nation’s Cybersecurity,” The White House, May 12, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.
- 4 David E. Sanger, Nicole Perlroth, and Julian E. Barnes. “As Understanding of Russian Hacking Grows, So Does Alarm,” *New York Times*, May 28, 2021, <https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html>; and David E. Sanger, “After Russian Cyberattack, Looking for Answers and Debating Retaliation,” *New York Times*, February 23, 2021, <https://www.nytimes.com/2021/02/23/us/politics/solarwinds-hack-senate-intelligence-russia.html>.
- 5 Andrew Archer et al., “Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor,” Mandiant, December 13, 2020, <https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor>.
- 6 Jon Porter, “White House now says 100 companies hit by Solar winds hit by Solar Winds hack, but more may be impacted,” *The Verge*, February 18, 2021, <https://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies>.

- 7 Kim Zetter, “DOJ Detected the SolarWinds Hack 6 Months Earlier than First Disclosed,” *Wired*, April 28, 2023, <https://www.wired.com/story/solarwinds-hack-public-disclosure/>.
- 8 Sanger, Perlroth, and Barnes, “As Understanding of Russian Hacking grows, So Does Alarm.”
- 9 Tim Starks and David DiMolfetta, “Years after discovery of Solar Winds breach, Russian hackers could be struggling,” *Washington Post*, April 25, 2023, <https://www.washingtonpost.com/politics/2023/04/25/years-after-discovery-solarwinds-breach-russian-hackers-could-be-struggling/>.
- 10 Tim Starks, “Feds aren’t well prepared to spot Solar Winds-style hacks at agencies, CISA official says,” *CyberScoop*, March 18, 2021, <https://cyberscoop.com/solarwinds-cisa-einstein-cdm-hsgac-wales/>.
- 11 Billy Mitchell, “CISA considering the future state of EINSTEIN as agencies modernize,” *FedScoop*, June 23, 2023, <https://fedscoop.com/cisa-considers-the-future-state-of-einstein-as-agencies-modernize/>.
- 12 “CISA’s Four-Part Plan to Spend \$650m on Cyber Protections,” *Federal News Network*, March 11, 2021, <https://federalnewsnetwork.com/cybersecurity/2021/03/cisas-four-part-plan-to-spend-650m-on-cyber-protections/>.
- 13 Sara Wilson, “Solar Winds recap: All of the federal agencies caught up in the Orion breach,” *FedScoop*, December 22, 2020, <https://fedscoop.com/solarwinds-recap-federal-agencies-caught-orion-breach/>.
- 14 Raphael Satter, Zeba Siddiqui, and James Pearson. “U.S. warns China could hack infrastructure, including pipelines, rail systems,” *Reuters*, May 26, 2023, <https://www.reuters.com/world/china/china-rejects-claim-it-is-spying-western-critical-infrastructure-2023-05-25/>.
- 15 David E. Sanger and Julian E. Barnes, “U.S. Hunts Chinese Malware That Could Disrupt American Military Operations,” *Washington Post*, July 29, 2023, <https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html>.
- 16 Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, April 1996).
- 17 Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York, NY: Oxford University Press, 2018); Erica D. Lonergan and Shawn W. Lonergan, *Escalation Dynamics in Cyberspace* (Oxford: Oxford University Press, 2023); Lucas Kello, *Striking Back: The End of Peace in Cyberspace - And How to Restore It* (New Haven, CT: Yale University Press, 2022); Eric Gartzke and Jon R. Lindsay, *Cross-Domain Deterrence: Strategy in an Era of Complexity* (Oxford: Oxford University Press, 2019); Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf; Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001); “Computational Propaganda,” Oxford Internet Institute, n.d., <https://www.oii.ox.ac.uk/research/projects/computational-propaganda/>; Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020); and Ben Buchanan, *The Cybersecurity Dilemma - Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2017).
- 18 Frank Bajak, “Microsoft: State-Sponsored Chinese Hackers Could Be Laying Groundwork for Disruption,” *AP News*, June 5, 2023, <https://apnews.com/article/microsoft-china-hacking-us-infrastructure-d4a4faefcc5d4d3c9f72e9acc24a71f9>.
- 19 Grace B. Mueller et al., *Cyber Operations during the Russo-Ukrainian War* (Washington, DC: CSIS, 2023), <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war>.
- 20 Dustin Volz and Jim Finkle, “U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam,” *Reuters*, March 24, 2016, <https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for->

hacking-dozens-of-banks-new-york-dam-idUSKCNOWQ1JF; Andy Greenberg, “Hackers Gain Direct Access to US Power Grid Controls,” *Wired*, September 6, 2017, <https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/>; Lucian Constantin, “North Korea’s Lazarus Group Hits Organizations with Two New Rats,” *CSO Online*, August 25, 2023, <https://www.csoonline.com/article/650413/north-koreas-lazarus-group-hits-organizations-with-two-new-rats.html>; Benjamin R. Young, “North Korea Knows How Important Its Cyberattacks Are,” *Foreign Policy*, February 9, 2022, <https://foreignpolicy.com/2022/02/09/north-korea-knows-how-important-its-cyberattacks-are/>; Nicole Perlroth, “Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say,” *New York Times*, July 6, 2017, <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html>; “Agriculture Industry on Alert after String of Cyber Attacks,” *GovTech*, June 14, 2022, <https://www.govtech.com/security/agriculture-industry-on-alert-after-string-of-cyber-attacks>; “Biggest Manufacturing Industry Cyber Attacks,” *Arctic Wolf*, March 12, 2023, <https://arcticwolf.com/resources/blog/top-8-manufacturing-industry-cyberattacks/>; Mariah Timms, “Murfreesboro Police, Fire Computers Hit by WannaCry Ransomware,” *Daily News Journal*, July 5, 2017, <https://www.dnj.com/story/news/crime/2017/07/05/murfreesboro-police-fire-computers-infected-virus/453774001/>; Andrew Liptak, “Hackers Are Holding San Francisco’s Muni Light-Rail System for Ransom,” *CNBC*, November 28, 2016, <https://www.cnn.com/2016/11/28/hackers-are-holding-san-franciscos-muni-light-rail-system-for-ransom.html>; Tom Polansek and Nandita Bose, “JBS Meat Plants Reopen as White House Blames Russia-Linked Group over Hack,” *Reuters*, June 3, 2021, <https://www.reuters.com/world/us/russia-linked-hacking-group-is-behind-cyberattack-against-jbs-bloomberg-news-2021-06-02/>; Jim Finkle, “Government Facilities Targets of Cyber Attacks,” *Reuters*, July 6, 2011, <https://www.reuters.com/article/us-usa-hackers/government-facilities-targets-of-cyber-attacks-idUSTRE7656M020110706>; Monica Pitrelli, “Leaked Documents Show Notorious Ransomware Group Has an HR Department, Performance Reviews and an ‘Employee of the Month’,” *CNBC*, April 14, 2022, <https://www.cnn.com/2022/04/14/conti-ransomware-leak-shows-group-operates-like-normal-tech-company.html>; Cluster25 Threat Intel, “Cybersecurity Risks and Challenges in the Chemical Industry,” *The Cluster25 Blog*, April 12, 2023, <https://blog.cluster25.duskriase.com/2023/04/12/cybersecurity-in-chemical-industry>; Adam Meyers, “Meet CrowdStrike’s Adversary of the Month for July: WICKED SPIDER,” *CrowdStrike*, July 26, 2018, <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/>; Ros Krasny, “Chinese Hacked U.S. Military Contractors, Senate Panel Finds,” *Reuters*, September 17, 2014, <https://www.reuters.com/article/us-usa-military-cyberspying/chinese-hackers-breach-u-s-military-contractors-senate-probe-idUSKBN0HC1TA20140917>; and Ryan Gallagher, “Chinese Hackers Compromised Telecom Firms, Researchers Say,” *Bloomberg*, August 4, 2021, <https://www.bloomberg.com/news/articles/2021-08-03/chinese-hackers-compromised-telecom-companies-researchers-say#xj4y7vzkg>.

- 21 National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS* (London: National Audit Office, April 2018), <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>.
- 22 Eduard Kovacs, “Flaw Found in OSISoft Product Deployed in Critical Infrastructure Sectors, Security,” *Security Week*, May 13, 2015, <https://www.securityweek.com/flaw-found-osisoft-product-deployed-critical-infrastructure-sectors/>.
- 23 Ionut Arghire, “Ransomware Targeted 14 of 16 U.S. Critical Infrastructure Sectors in 2021,” *Security Week*, February 10, 2022, <https://www.securityweek.com/ransomware-targeted-14-16-us-critical-infrastructure-sectors-2021/>.
- 24 Jonathan Reed, “High-impact attacks on critical infrastructure climb 140%,” *Security Intelligence*, June 26, 2023, <https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/>.
- 25 Manuel Castells, *The Information Age: Economy, Society and Culture Vol. I—The Rise of the Network Society* (Cambridge, MA and Oxford, UK: Blackwell, 1996); Manuel Castells, *The Information Age:*

Economy, Society and Culture Vol. II—The Power of Identity (Cambridge, MA and Oxford, UK: Blackwell, 1997); Manuel Castells, *The Information Age: Economy, Society and Culture Vol. III—End of Millennium* (Cambridge, MA and Oxford, UK: Blackwell, 1998); and Jeremy Black, *The Power of Knowledge: How Information and Technology Made the Modern World* (New Haven, CT: Yale University Press, 2015), <https://yalebooks.yale.edu/9780300208672/the-power-of-knowledge>.

- 26 Richard E. Lee, *Longue Duree and World-Systems Analysis* (Albany, NY: State University of New York Press, 2013).
- 27 Rebecca Bales, “The First Computer Virus of Bob Thomas Explained: Everything You Need to Know,” *Computer History*, August 21, 2023, <https://history-computer.com/the-first-computer-virus-of-bob-thomas/>.
- 28 Jan Kopriva, “50 years of malware? Not really. 50 years of computer worms? That is a different story,” *SANS Internet Storm Center*, March 16, 2021, <https://isc.sans.edu/diary/rss/27208>.
- 29 “About NSF,” National Science Foundation (NSF), n.d., <https://new.nsf.gov/about>.
- 30 “ARPANET,” Defense Advanced Research Projects Agency, n.d., https://www.darpa.mil/attachments/ARPANET_final.pdf.
- 31 “1980s,” NSF, n.d., https://www.nsf.gov/news/special_reports/nsf-net/1980.jsp.
- 32 “NSF and the Birth of the Internet,” NSF, n.d., https://www.nsf.gov/news/special_reports/nsf-net/1980s.jsp; and Peter J. Denning, Anthony Hearn, and C. William Kern, “History and Overview of CSNET,” in David C. Wood and Simon S. Lam, eds. *SIG COMM ’83: Proceedings of the Symposium on Communications Architectures & Protocols* (New York, NY: Association for Computing Machinery, October 1983), 138-145, doi:10.1145/1035237.1035267.
- 33 D.A. Grier and M. Campbell, “A Social History of Bitnet and Listserv, 1985-1991,” *IEEE Annals of the History of Computing* 22, No. 2 (2000): 32-41, doi: 10.1109/85.841135.
- 34 “1980s,” NSF.
- 35 Subcommittee on Transportation, Aviation, and Materials, *Computer and Communications Security and Privacy* (Washington, DC: U.S. Government Printing Office, April 1984), 18-19, <https://www.ojp.gov/pdffiles1/Digitization/95323NCJRS.pdf>.
- 36 John Markoff, “Breach Reported in U.S. Computers,” *New York Times*, April 18, 1988, <https://www.nytimes.com/1988/04/18/us/breach-reported-in-us-computers.html>.
- 37 Ibid.; and Clifford Stoll, “Stalking the Wily Hacker,” *Communications of the ACM* 31, no. 5 (May 1988): 484, 488, <https://dl.acm.org/doi/pdf/10.1145/42411.42412>.
- 38 Markoff, “Breach Reported in U.S. Computers.”
- 39 Stoll, “Stalking the Wily Hacker,” 486.
- 40 Ibid., 487.
- 41 “2W. Germans Get Suspended Terms as Computer Spies,” *LA Times*, February 16, 1990, <https://www.latimes.com/archives/la-xpm-1990-02-16-mn-667-story.html>.
- 42 Department of Defense (DOD) Computer Security Center, *Department of Defense Trusted Computer System Evaluation* (Washington, DC: DOD, August 1983), 1, <https://apps.dtic.mil/sti/citations/ADA477648>.
- 43 “DoD Directive 5215.1: Computer Security Evaluation Center,” DOD, October 25, 1982, <https://www.hsdl.org/c/view?docid=444>.
- 44 See NSA/NCSC Rainbow Series hosted by the Federation of American Scientists, <https://irp.fas.org/nsa/>

rainbow.htm.

- 45 Maurice Matloff and Edwin Marion Snell, *Strategic Planning for Coalition Warfare, 1941-1942* (Washington, DC: Office of the Chief of Military History, Department of the Army, 1953).
- 46 DOD, *Department of Defense Trusted Computer System Evaluation Criteria* (Washington, DC: DOD, December 1985), <https://irp.fas.org/nsa/rainbow/std001.htm>.
- 47 David Bailey, "Attacks on Computers: Congressional Hearings and Pending Legislation," IEEE, April 29, 1984, 186, <https://ieeexplore.ieee.org/document/6234796>.
- 48 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), <https://www.congress.gov/99/statute/STATUTE-100/STATUTE-100-Pg1848.pdf>. In particular, see Section 2, d) New Offenses, and (4).
- 49 John Leyden, "That Time When an NSA Bloke's Son Borked the Entire Internet," The Register, November 18, 2013, https://www.theregister.com/2013/11/04/morris_worm_anniversary/; and "The Morris Worm," FBI, November 2, 2018, <https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218>.
- 50 National Defense Authorization Act for Fiscal Year 1966, Pub. L. No. 104-106, 110 Stat. 186 (1996), <https://www.congress.gov/104/plaws/publ106/PLAW-104publ106.pdf>. In particular, see Division E: Information Technology Management Reform.
- 51 Ibid., Section 5125: Agency Chief Information Officer.
- 52 Ibid., Section 5124: Acquisitions of Information Technology.
- 53 "PDD-63 - Critical Infrastructure Protection," The White House, May 22, 1988, <https://clinton.presidentiallibraries.us/items/show/12762>.
- 54 Ibid.
- 55 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>. See Section 1030(e) for the revised definition of a protected computer and section 1030(a)(5) for computers used for national defense or security.
- 56 "About E-Gov," E-Gov, n.d., <https://georgewbush-whitehouse.archives.gov/omb/egov/g-1-background.html>; and E-Government Act of 2002, Pub. L. 107-347, 116 Stat. 2899 (2002), <https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>.
- 57 Federal Information Security Management Act of 2002, H.R. 3844, 107th Cong. (2002), <https://www.congress.gov/bill/107th-congress/house-bill/3844>.
- 58 Chris Jaikaran, *Federal Cybersecurity: Background and Issues for Congress*, CRS Report No. R46926 (Washington, DC: Congressional Research Service, September 2021), 11, <https://crsreports.congress.gov/product/pdf/R/R46926>.
- 59 The White House, *The National Strategy to Secure Cyberspace* (Washington, DC: White House, February 2003), https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.
- 60 Office of Management and Budget, *FY 2002 Report to Congress on Federal Government Information Security Reform* (Washington, DC: OMB, May 2003), 4, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/inforeg/2002gisra_report.pdf.
- 61 U.S. Government Accountability Office, "Gao-16-140T, National Protection and Programs Directorate: Factors to Consider When Reorganizing," gao.gov, October 7, 2015, <https://www.gao.gov/assets/gao-16-140t.pdf>.

- 62 U.S. Department of Homeland Security, “Brief Documentary History of the Department of Homeland Security,” Homeland Security Digital Library, 2008, www.hsdl.org.
- 63 The White House, *Cyberspace Policy Review* (Washington, DC: White House, 2009), <https://irp.fas.org/eprint/cyber-review.pdf>.
- 64 The White House, *National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)* (Washington, DC: White House, January 2008), <https://irp.fas.org/offdocs/nspd/nspd-54.pdf>.
- 65 James Andrew Lewis, *Securing Cyberspace for the 44th Presidency* (Washington, DC: CSIS, December 2008), <https://www.csis.org/analysis/securing-cyberspace-44th-presidency>.
- 66 “Continuous Diagnostics and Mitigation (CDM) Program,” CISA, n.d., <https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program>; and “EINSTEIN,” CISA, n.d., <https://www.cisa.gov/einstein>.
- 67 U.S. Department of Homeland Security, *Cyber and Infrastructure Protection Transition Way Ahead* (Washington, DC: Department of Homeland Security, March 2016), <https://www.scribd.com/doc/305423245/Nppd-Transition-3-17-16-Final>.
- 68 Cynthia Brumfield, “What is the CISA? How the new federal agency protects critical infrastructure from cyber threats,” CSO, July 1, 2019, <https://www.csoonline.com/article/567457/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html>.
- 69 David Petraeus and Kiran Sridhar, “The Case for a National Cybersecurity Agency,” *Politico*, September 5, 2018, <https://www.politico.com/agenda/story/2018/09/05/cybersecurity-agency-homeland-security-000686/>.
- 70 The White House, *National Cyber Strategy of the United States of America* (Washington, DC: White House, September 2018), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
- 71 Brumfield, “What is the CISA?”
- 72 Valeriano and Jensen, “Building a National Cyber Strategy”; and Montgomery et al., *Cyberspace Solarium Commission Report*.
- 73 The White House, *National Cybersecurity Strategy* (Washington, DC: White House, March 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.
- 74 The White House, *National Cybersecurity Strategy Implementation Plan* (Washington, DC: White House, July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.
- 75 “Executive Order on Improving the Nation’s Cybersecurity,” The White House, May 12, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-onimproving-the-nations-cybersecurity/>.
- 76 Emily Harding et al., “‘Never Trust, Always Verify’: Federal Migration to ZTA and Endpoint Security,” CSIS, *CSIS Briefs*, June 16, 2022, 6, <https://www.csis.org/analysis/never-trust-always-verify-federal-migration-zta-andendpoint-security>.
- 77 Strengthening American Cybersecurity Act of 2002, S. 3600, 117th Cong. (2002), <https://www.congress.gov/bill/117th-congress/senate-bill/3600/text>.
- 78 John Hewitt Jones, “FISMA Reform Bill Advances in Senate,” FedScoop, July 26, 2023, <https://fedscoop.com/fisma-reform-bill-advances-in-senate/>.

- 79 CISA, *Strategic Plan 2023-2025* (Washington, DC: CISA, September 2022), <https://www.cisa.gov/strategic-plan>; and CISA, *Strategic Plan FY2024-2026* (Washington, DC: CISA, August 2023), https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf.
- 80 CISA, *CISA 2022 Year in Review* (Washington, DC: CISA, 2022), https://www.cisa.gov/sites/default/files/publications/CISA-YearInReview_v1_508.pdf.
- 81 “National Cybersecurity Protection System,” CISA, n.d., <https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system>.
- 82 John Curran, “MeriTalk Q&A: CISA’s Hartman Talks the Birth of CADS, Evolution of EINSTEIN,” MeriTalk, April 21, 2023, <https://www.meritalk.com/articles/meritalk-qa-cisa-hartman-talks-the-birth-of-cads-evolution-of-einstein/>.
- 83 Justin Doubleday, “CISA lays out post-EINSTEIN future with shift to ‘Cyber Analytics and Data System,’” Federal News Network, March 17, 2023, <https://federalnewsnetwork.com/cybersecurity/2023/03/cisa-lays-out-post-einstein-future-with-shift-to-cyber-analytics-and-data-system/>.
- 84 CISA, *Budget Overview: Fiscal Year 2024* (Washington, DC: CISA, 2023), 10, <https://www.dhs.gov/sites/default/files/2023-03/CYBERSECURITY%20AND%20INFRASTRUCTURE%20SECURITY%20AGENCY.pdf>; and John Curran, “CISA’s EINSTEIN Gets Extension in FY2023 Approps Bill,” MeriTalk, December 21, 2022, <https://www.meritalk.com/articles/cisas-einstein-gets-extension-in-fy2023-approps-bill/>.
- 85 CISA, *Budget Overview: FY 2024*.
- 86 Curran, “MeriTalk Q&A.”
- 87 “Protective Domain Name System (DNS) Resolver Service,” CISA, n.d., https://www.cisa.gov/sites/default/files/publications/FINAL-CSSO-Protective_DNS-Fact_Sheet.pdf.
- 88 CISA, *CISA 2022 Year in Review*, 4; and Montgomery et al., *Cyberspace Solarium Commission Report*.
- 89 Consolidated Appropriations Act, Pub. L. 117-103, 136 Stat 49 (2022), <https://www.congress.gov/bill/117th-congress/house-bill/2471/text>.
- 90 “Cyber Incident Reporting for Critical Infrastructure Act of 2022,” CISA, n.d., <https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia>.
- 91 George Platsis, “What CISOs Should Know about CIRCIA Incident Reporting,” Security Intelligence, December 8, 2022, <https://securityintelligence.com/articles/what-cisos-should-know-circia-incident-reporting/>; and Cynthia Brumfield, “No consensus on creating a unified US cyber incident reporting framework,” CSO, June 29, 2023, <https://www.csoonline.com/article/644155/creating-a-unified-cyber-incident-reporting-framework-will-be-no-easy-feat.html>.
- 92 CISA, *Budget Overview: FY 2024*.
- 93 Jane Edwards, “CISA’s Michael Duffy on Continuous Diagnostics & Mitigation Program,” ExecutiveGov, July 24, 2023, <https://executivegov.com/2023/07/cisas-michael-duffy-on-continuous-diagnostics-and-mitigation-program/>.
- 94 “CDM Program,” CISA.
- 95 Akhilomen Oniha et al., “Information Security Continuous Monitoring (ISCM),” CSIAC, 2017, <https://csiic.org/articles/information-security-continuous-monitoring-iscm/4/>.
- 96 “CDM Program Overview,” CISA, 2020, https://www.cisa.gov/sites/default/files/publications/2020%2009%20003_CDM%20Program%20Overview_Fact%20Sheet_1.pdf.

- 97 This new approach differs from the past when each agency internally developed its own dashboard or monitoring capability. For example, the DHS created an internal dashboard architecture known as the Continuous Monitoring as a Service (CMaaS) Program, which powered a continuous monitoring tool kit, integrating services for the planning, provisioning, operation, and management of tools, sensors, dashboards, and data feeds.
- 98 “CDM Program Overview,” CISA.
- 99 “BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks,” CISA, News release, October 3, 2022, <https://www.cisa.gov/news-events/directives/binding-operational-directive-23-01>.
- 100 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388 (2021), <https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf>. See in particular Sec. 1739, “Assessment on Defense Industrial Base Cybersecurity Threat Hunting Program.”
- 101 Jen Easterly, *CISA 2025: The State of American Cybersecurity from CISA's Perspective* (Washington, DC: Committee on Homeland Security, April 2023), https://democrats-homeland.house.gov/imo/media/doc/easterly_testimony_cip_042723.pdf.
- 102 “CDM Program Overview,” CISA.
- 103 Justin Doubleday, “CISA sees uptick in agencies automatically reporting into CDM dashboard,” Federal News Network, July 7, 2023, <https://federalnewsnetwork.com/cybersecurity/2023/07/cisa-sees-uptick-in-agencies-automatically-reporting-into-cdm-dashboard/>.
- 104 “CDM: The Multitool in your Cyber Kit,” MeriTalk, 2022, <https://meritalk.com/study/cdm-the-multitool/?campaign=editorial>.
- 105 Richard Bejtlich, “Become a Hunter,” *Information Security* 13, no. 6 (July/August 2011), http://docs.media.bitpipe.com/io_24x/io_24618/item_370437/informationsecurity_july_aug2011_final.pdf.
- 106 Richard Bejtlich, “The Origin of Threat Hunting,” TaoSecurity, March 2017, <https://taosecurity.blogspot.com/2017/03/the-origin-of-threat-hunting.html>.
- 107 Ibid.
- 108 “Mitre ATT&CK® Framework,” MITRE ATT&CK, n.d., <https://attack.mitre.org/>.
- 109 For an overview of threat hunt, see “What Is Cyber Threat Hunting? [Proactive Guide],” CrowdStrike, August 9, 2023, <https://www.crowdstrike.com/cybersecurity-101/threat-hunting/>.
- 110 CISA, “Helping Cyber Defenders ‘Decide’ to Use Mitre ATT&CK: CISA,” News release, August 28, 2023, <https://www.cisa.gov/news-events/news/helping-cyber-defenders-decide-use-mitre-attck>; “Threat Hunting - a Cybersecurity Paradigm Shift,” Infosys, n.d., <https://www.infosys.com/insights/cyber-security/threat-hunting.html>; and “Cyber Threat Hunting at Scale across .Gov,” Booz Allen Hamilton, July 7, 2022, <https://www.boozallen.com/expertise/cybersecurity/how-to-hunt-cyber-threats-at-scale-across-gov.html>.
- 111 “CISA Releases Hunt Tool for Microsoft’s Cloud Services,” Dark Reading, March 28, 2023, <https://www.darkreading.com/dr-tech/cisa-releases-hunt-tool-for-microsoft-s-cloud-services>.
- 112 Michael McLaughlin, “Reforming FedRAMP: A Guide to Improving the Federal Procurement and Risk Management of Cloud Services,” Information Technology and Innovation Foundation, June 3, 2022, <https://itif.org/publications/2020/06/15/reforming-fedramp-guide-improving-federal-procurement-and-risk-management/>.
- 113 “FedRAMP Security Assessment Framework,” FedRAMP, November 15, 2017.

- 114 General Services Administration, “FedRAMP Authorizations Hit 300 Milestone,” FedRAMP, April 26, 2023, <https://www.fedramp.gov/2023-04-26-fedramp-authorizations-hit-300/>.
- 115 Billy Mitchell, “New FedRAMP guidance forthcoming as the cloud marketplace evolves,” FedScoop, September 8, 2023, <https://fedscoop.com/new-fedramp-guidance-forthcoming-as-the-cloud-marketplace-evolves/>.
- 116 CISA, “BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities,” News release, November 3, 2021, <https://www.cisa.gov/news-events/directives/binding-operational-directive-22-01>.
- 117 “Kev Catalog Reaches 1000, What Does That Mean and What Have We Learned : CISA,” CISA, October 5, 2023, <https://www.cisa.gov/news-events/news/kev-catalog-reaches-1000-what-does-mean-and-what-have-we-learned>; and Jacob Baines, “The VulnCheck 2022 Exploited Vulnerability Report - A Year Long Review of the CISA KEV Catalog,” VulnCheck, March 2, 2023, <https://vulncheck.com/blog/2022-cisa-kev-review>.
- 118 Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073 (2014), <https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf>. See section 3553, “Authority and functions of the Director and the Secretary.”
- 119 Jacob Baines, “The VulnCheck 2022 Exploited Vulnerability Report - A Year Long Review of the CISA KEV Catalog,” VulnCheck, March 2, 2023, <https://vulncheck.com/blog/2022-cisa-kev-review>.
- 120 CISA, *Strategic Plan FY2024-2026*.
- 121 Montgomery et al., *Cyberspace Solarium Commission Report*.
- 122 “Joint Cyber Defense Collaborative,” CISA, n.d., <https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative>.
- 123 Lamar Johnson, “CISA Director Easterly Talks JCDC, Importance of Cyber Collaboration,” MeriTalk, September 28, 2021, <https://www.meritalk.com/articles/cisa-director-easterly-talks-jcdc-importance-of-cyber-collaboration/>.
- 124 “Joint Cyber Defense Collaborative,” CISA.
- 125 “CISA Expands the Joint Cyber Defense Collaborative to Include Industrial Control Systems Industry Expertise,” CISA, News release, April 20, 2022, <https://www.cisa.gov/news-events/news/cisa-expands-joint-cyber-defense-collaborative-include-industrial-control-systems>.
- 126 Cate Burgan, “CISA’s JCDC Leveraging Global Partnerships to Protect U.S. Assets,” MeriTalk, December 14, 2022, <https://www.meritalk.com/articles/cisas-jcdc-leveraging-global-partnerships-to-protect-u-s-assets/>.
- 127 Natalie Alms, “Industry reps like CISA’s public-private cybersecurity collaborative, but offer tips on how to scale it,” NextGov/FCW, March 23, 2023, <https://www.nextgov.com/cybersecurity/2023/03/industry-reps-cisas-public-private-cybersecurity-collaborative-offer-tips-how-scale-it/384379/>.
- 128 Ibid.
- 129 CISA, *Federal Government Incident and Vulnerability Response Playbooks* (Washington, DC: CISA, November 2021), <https://www.cisa.gov/sites/default/files/2023-02/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks-508c.pdf>.
- 130 “Incident Response Training,” CISA, n.d., <https://www.cisa.gov/resources-tools/programs/Incident-Response-Training>.
- 131 “Cybersecurity Incident Response,” CISA, n.d., <https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response>.
- 132 Emily Harding and Suzanne Spaulding, “Threats Happen; Consequences Don’t Have To,” CSIS,

- Commentary, July 11, 2023, <https://www.csis.org/analysis/threats-happen-consequences-dont-have>.
- 133 Ibid.
- 134 Hadeil Ali et al., *Innovation for Resilience* (Washington, DC: CSIS, March 2023), 1, <https://www.csis.org/analysis/innovation-resilience>.
- 135 “Cyber Storm: Securing Cyber Space,” CISA, n.d., <https://www.cisa.gov/cyber-storm-securing-cyber-space>.
- 136 “Cyber Storm IX: National Cyber Exercise,” CISA, n.d., <https://www.cisa.gov/cyber-storm-ix-national-cyber-exercise>.
- 137 CISA, “CISA Releases Second Version of Guidance for Secure Migration to the Cloud,” News release, June 23, 2022, <https://www.cisa.gov/news-events/news/cisa-releases-second-version-guidance-secure-migration-cloud>; and “Zero Trust Maturity Model,” CISA, n.d., <https://www.cisa.gov/zero-trust-maturity-model>.
- 138 CISA, *Cyber Safety Review Board Charter* (Washington, DC: CISA, September 2021), https://www.cisa.gov/sites/default/files/publications/Cyber%20Safety%20Review%20Board%20Charter_508%20Compliant.pdf.
- 139 “CSRB Review: December 2021 LOG4J Event,” Cyber Safety Review Board, n.d., <https://www.cisa.gov/sites/default/files/publications/CSRB-Log4J-Key-Findings-and-Recommendations-Summary-508c.pdf>; and DHS, “Cyber Safety Review Board Releases Report on Activities of Global Extortion-Focused Hacker Group Lapsus\$,” Press release, August 10, 2023, <https://www.dhs.gov/news/2023/08/10/cyber-safety-review-board-releases-report-activities-global-extortion-focused>.
- 140 “Department of Homeland Security’s Cyber Safety Review Board to Conduct Review on Cloud Security,” DHS, Press release, August 11, 2023, <https://www.dhs.gov/news/2023/08/11/departement-homeland-securitys-cyber-safety-review-board-conduct-review-cloud>.
- 141 “CSRB Review: December 2021 LOG4J Event,” Cyber Safety Review Board.
- 142 Tarah Wheeler and Adam Shostak, “The Cyber Safety Review Board Should Investigate Major Historical Incidents,” Council on Foreign Relations, May 25, 2023, <https://www.cfr.org/blog/cyber-safety-review-board-should-investigate-major-historical-incidents>.
- 143 Consolidated Appropriations Act, 2021, Pub. L. 116-260, 134 Stat. 1182 (2020), <https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf>. See in particular Title IX, DOTGOV Act of 2020.
- 144 Ibid., Sec. 902 Findings, (5).
- 145 For a registrar-suggested template, see “Authorization letter template: Federal,” .gov, <https://get.gov/registration/authorization-templates/federal/>. For the online form, see “.gov Registrar,” .gov, https://domains.dotgov.gov/dotgov-web/welcome.xhtml?_m=1&OWASP-CSRF_TOKEN=UASE-FG09-OAOT-V9PC-96A2-8J50-OTVH-VIDA.
- 146 Consolidated Appropriations Act. See Sec. 2215 (b) Availability of .gov domain (2), (c) Requirements, and (d) Executive Branch.
- 147 “.gov is Moving to CISA,” .gov, March 8, 2021, <https://get.gov/2021/3/8/moving-to-cisa/>.
- 148 Consolidated Appropriations Act. See Section 902 Findings (4).
- 149 “Memorandum for the Heads of Executive Departments and Agencies,” Office of Management and Budget, February 8, 2023, 1, <https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-10-DOTGOV-Act-Guidance.pdf>.
- 150 “Registration,” .gov, n.d., <https://get.gov/registration/#new-to-gov>; and “Domain Security Best Practices,” .gov, n.d., <https://get.gov/help/security-best-practices/>.

- 151 “Cyber Resource Hub,” CISA, n.d., <https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services>. As of June 2023, CISA advertises scanning at no cost. “Cyber Hygiene Services,” CISA, n.d., <https://www.cisa.gov/cyber-hygiene-services>.
- 152 Ines Kagubare, “House subcommittee approves \$334 million funding bump for CISA,” *The Hill*, June 16, 2022, <https://thehill.com/policy/cybersecurity/3526827-house-subcommittee-approves-334-million-funding-bump-for-cisa/>.
- 153 Christian Vasquez, “CISA Director Says Cutting Agency’s Budget Would Return It to ‘Pre-SolarWinds World’,” *CyberScoop*, March 28, 2023, <https://cyberscoop.com/easterly-cisa-budget-china-biden>.
- 154 Harding et al., “‘Never Trust, Always Verify’.”
- 155 “Strengthening America’s Cyber Resiliency: A Conversation with the National Cyber Director,” YouTube video, posted by FDD, June 2, 2022, 1:00:40, <https://www.youtube.com/watch?v=dxqo1OCKArw>; “Strengthening America’s Cyber Resiliency: A Conversation with the National Cyber Director,” Foundation for Defense of Democracies, June 2, 2022, <https://www.fdd.org/wp-content/uploads/2022/06/Transcript-strengthening-americas-cyber-resiliency.pdf>.
- 156 “Department of Justice (DOJ)—A Shared Service Provider,” CISA, n.d., <https://www.cisa.gov/resources-tools/programs/cybersecurity-quality-services-management-office-qsmo/shared-service-provider-department-justice-doj>.
- 157 “Cyber Marketplace,” CISA, n.d., <https://www.cisa.gov/resources-tools/programs/cyber-marketplace>.
- 158 CISA, *Strategic Plan FY2024-2026*.
- 159 White House, *National Cybersecurity Strategy*, 13.
- 160 Full details of the tabletop exercise and public survey methodology will be published as a follow-up report on the CSIS website.
- 161 Chi-square p-value: 4.855×10^{-54} . 855×10^{-5} (or 0.00004855).
- 162 Di Cooke, Abigail Edwards, Sophia Barkoff, and Kathryn Kelly, “As Good As a Coin Toss: Human detection of AI-generated images, videos, audio, and audiovisual content,” arXiv preprint, submitted in 2023.
- 163 Nina Jankowicz, “I Shouldn’t Have to Accept Being in Deepfake Porn,” *The Atlantic*, June 25, 2023, <https://www.theatlantic.com/ideas/archive/2023/06/deepfake-porn-ai-misinformation/674475/>.
- 164 Zhanna L. Malekos Smith, “Closing the barn door on ‘store now, decrypt later’ attacks,” *The Hill*, November 5, 2022, <https://thehill.com/opinion/cybersecurity/3719786-closing-the-barn-door-on-store-now-decrypt-later-attacks>.
- 165 Sanger and Barnes, “U.S. Hunts Chinese Malware.”
- 166 Derek B. Johnson, “Inglis: There may not be one throat to choke in the cyber hierarchy,” *Scmagazine*, April 13, 2022, <https://www.scmagazine.com/analysis/inglis-there-may-not-be-one-throat-to-choke-in-the-cyber-hierarchy>.
- 167 Cyberspace Solarium Commission, *Growing a Stronger Federal Cyber Workforce* (Washington, DC: Cyberspace Solarium Commission, September 2020), <https://cybersolarium.org/white-papers/growing-a-stronger-federal-cyber-workforce>.
- 168 The White House, *National Cyber Workforce and Education Strategy: Unleashing America’s Cyber Talent* (Washington, DC: White House, July 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf>.
- 169 “Confidence in Institutions,” Gallup, updated 2023, <https://news.gallup.com/poll/1597/confidence->

institutions.aspx.

- 170 Grace Dille, “CISA Rolling out Joint Collaborative Environment to Enrich Threat Data,” MeriTalk, July 17, 2023, <https://www.meritalk.com/articles/cisa-rolling-out-joint-collaborative-environment-to-enrich-threat-data/>.
- 171 Kathleen Hicks, “Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DoD Field Activity Directors,” DOD, August 10, 2023, https://media.defense.gov/2023/Aug/10/2003279040/-1/-1/1/ESTABLISHMENT_OF_CDAO_GENERATIVE_AI_AND_LARGE_LANGUAGE_MODELS_TASK_FORCE_TASK_FORCE_LIMA_OSD006491-23_RES_FINAL.PDF.
- 172 DHS, *Harmonization of Cyber Incident Reporting to the Federal Government* (Washington, DC: DHS, September 2023), <https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government>.
- 173 Ibid., 26.
- 174 Ibid., E-1.
- 175 Evan Schuman, “CISOs Need Backing To Take Charge of Security,” The Edge, August 2, 2023, <https://www.darkreading.com/edge-articles/cisos-need-backing-to-take-charge-of-security>.
- 176 Harding et al., “‘Never Trust, Always Verify’.”
- 177 “Cyber Marketplace,” CISA, n.d., <https://www.cisa.gov/resources-tools/programs/cyber-marketplace>.
- 178 “JCDC Success Stories,” CISA, n.d., <https://www.cisa.gov/topics/partnerships-and-collaboration/jcdc-success-stories>.
- 179 Jim Lewis, “Cyber Workforce Strategies Should Produce at Scale,” CSIS, *Commentary*, August 22, 2022, <https://www.csis.org/analysis/cyber-workforce-strategies-should-produce-scale>; and Mark Britton, “Does the White House’s National Cyber Workforce and Education Strategy Go Far Enough?,” Infosecurity Magazine, August 10, 2023, <https://www.infosecurity-magazine.com/opinions/white-house-cyber-workforce/>.
- 180 White House, *National Cyber Workforce and Education Strategy*.
- 181 Ibid., 57.
- 182 Ibid.
- 183 “Biden-Harris Administration Announces National Cyber Workforce and Education Strategy, Unleashing America’s Cyber Talent,” The White House, Fact sheet, July 31, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-%E2%81%A0harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent/>; and Dina Temple-Raston and Will Jarvis, “‘A nerd’s gotta do what a nerd’s gotta do:’ Why Craig Newmark is funding a cyber civil defense,” Recorded Future, August 19, 2022, <https://therecord.media/a-nerds-gotta-do-what-a-nerds-gotta-do-why-craig-newmark-is-funding-a-cyber-civil-defense>.
- 184 Dawn Nuschler, *Inflation-Indexing Elements in Federal Entitlement Programs*, CRS Report No. R42000 (Washington, DC: Congressional Research Service, April 2013), <https://crsreports.congress.gov/product/pdf/R/R42000>.
- 185 “Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by Ai,” The White House, July 21, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/>.
- 186 The Office of Management and Budget (OMB), the Federal CDO Council, and U.S. General Services Administration, *Federal Data Strategy 2021 Action Plan* (Washington, DC: OMB, 2021), <https://strategy.data.gov/assets/docs/2021-Federal-Data-Strategy-Action-Plan.pdf>; National Security Commission on

Artificial Intelligence, *Final Report: National Security Commission on Artificial Intelligence* (Washington, DC: National Security Commission on Artificial Intelligence, 2021), <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf>; National Artificial Intelligence Research Resource Task Force, *Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem An Implementation Plan for a National Artificial Intelligence Research Resource* (Alexandria, VA: NSF, January 2023), <https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf>; and National Institute of Standards and Technology, *AI Risk Management Framework* (Gaithersburg, MD: National Institute of Standards and Technology, March 2023), <https://www.nist.gov/itl/ai-risk-management-framework>.

- 187 Daniel Fabian, “Google’s AI Red Team: The Ethical Hackers Making Ai Safer,” Google, July 19, 2023, <https://blog.google/technology/safety-security/googles-ai-red-team-the-ethical-hackers-making-ai-safer/>; Ram Shankar Siva Kumar, “Microsoft AI Red Team Building Future of Safer Ai,” Microsoft Security Blog, August 7, 2023, <https://www.microsoft.com/en-us/security/blog/2023/08/07/microsoft-ai-red-team-building-future-of-safer-ai/>; and Christopher Burgess, “Hacking the Future: Notes from DEF CON’s Generative Red Team Challenge,” CSO Online, August 28, 2023, <https://www.csoonline.com/article/650365/hacking-the-future-notes-from-the-generative-red-team-challenge-at-def-con-31.html>.
- 188 Amir Shachar, “Is Bias in AI Algorithms a Threat to Cloud Security?,” Dark Reading, August 25, 2023, <https://www.darkreading.com/cloud/is-bias-in-ai-algorithms-a-threat-to-cloud-security>.
- 189 Dominik Sowinski, “Cloud Security in the Era of Artificial Intelligence,” Security Intelligence, September 27, 2023, <https://securityintelligence.com/posts/cloud-security-in-the-era-of-artificial-intelligence/>; and Sue Poremba et al., “How Generative AI Is a Game Changer for Cloud Security,” TechRepublic, June 30, 2023, <https://www.techrepublic.com/article/generative-ai-cloud-security/>.
- 190 “U.S. Cyber Command History,” U.S. Cyber Command, accessed October 5, 2023, <https://www.cybercom.mil/About/History/>.
- 191 “History: Joint Force Headquarters - Department of Defense Information Network,” DOD, accessed October 5, 2023, <https://www.jfhq-dodin.mil/About-Us/History>.
- 192 “Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) Concept of Operations {CONOPS},” U.S. Cyber Command, 2014, https://www.cybercom.mil/Portals/56/Documents/FOIA%20Reading%20Room%20Docs/RELEASED%20DOCUMENTS/2014-00-00_JFHQ-DODIN_Concept_of_Operations.pdf.
- 193 Cheryl Pellerin, “Rogers: Cybercom Defending Networks, Nation,” DOD, August 18, 2014, <https://www.defense.gov/News/News-Stories/Article/Article/603083/>; and G. Alexander Crowther and Shaheen Ghori, “Detangling the Web: A Screenshot of U.S. Government Cyber Activity,” National Defense University Press, July 1, 2015, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/607658/detangling-the-web-a-screenshot-of-us-government-cyber-activity/>.
- 194 CISA, “CISA Announces Transfer of the .Gov Top-Level Domain from U.S. General Services Administration: CISA,” Press release, September 29, 2023, <https://www.cisa.gov/news-events/news/cisa-announces-transfer-gov-top-level-domain-us-general-services-administration>.
- 195 Government Accountability Office, *DOD CYBERSECURITY Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared* (Washington, DC: Government Accountability Office, November 2022), <https://www.gao.gov/assets/gao-23-105084.pdf>.
- 196 Kevin Townsend, “Cisa Introduces Secure-by-Design and Secure-by-Default Development Principles,” SecurityWeek, April 14, 2023, <https://www.securityweek.com/cisa-introduces-secure-by-design-and-secure-by-default-development-principles/>.
- 197 Benjamin Jensen, Brandon Valeriano, and Mark Montgomery, “The Strategic Implications of SolarWinds,” Lawfare, December 18, 2020, <https://www.lawfareblog.com/strategic-implications-solarwinds>.

COVER PHOTO VIDEOFLOW/ADOBE STOCK



1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.csis.org