U.S. DEPARTMENT OF ENERGY

Cybersecurity Strategy

January 2024

Table of Contents

Message from the Deputy Secretary

Cybersecurity is a top priority of this Administration. In May 2021, President Biden issued Executive Order 14028, *Improving the Nation's Cybersecurity*, which makes a significant contribution towards the modernization of cybersecurity defenses by protecting federal networks, improving information-sharing between the United States Government and the private sector on cyber data, and strengthening our ability to respond to security incidents when they occur.

In July 2021, the President issued a *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*, which reinforced the importance of working with critical infrastructure owners and operators to address cyber threats facing sectors that operate industrial control systems (ICS).

In March 2023, the White House released the *National Cybersecurity Strategy*, which emphasizes an approach to a collective defense in which the United States will work with its allies and partners to advance our digital ecosystem, increasing its defensibility, resiliency, and alignment with American values.

The Department of Energy (DOE) is approaching the cybersecurity challenge as an enterprise-wide effort, incorporating both assets and capabilities from across our program offices as well as our National Laboratories. This *DOE Cybersecurity Strategy* not only focuses attention on protecting DOE's federal systems and assets, but also on protecting our Nation's critical energy infrastructure. Cybersecurity is not just an area of concern for the Office of the Chief Information Officer (OCIO) and the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), it is essential to both the Department's daily operations and to ensure the flow of electricity, oil, and natural gas across the country for millions of Americans. This strategy attempts to align the mission and cybersecurity goals across the Department. It is a crucial roadmap for how to translate our priorities into action to protect the Department and the U.S. energy sector's most valuable assets. Cybersecurity is a collective effort, requiring significant partnership and collaboration. Success will require sustained resources, energy, focus, persistence, and practice.

In my role as chair of the DOE Cyber and Information Technology (IT)/Operational Technology (OT) Executive Council, I have had the privilege of meeting and working with IT and cybersecurity policy and technical leaders across the Department to advance a holistic approach to cybersecurity. This strategy defines several specific objectives which we must accomplish to ensure the continued success of our collective cybersecurity efforts. These include identifying our cybersecurity risk, mitigating that risk, enabling mission resilience, developing the cybersecurity workforce, and protecting our Nation's critical energy infrastructure.

Cybersecurity is a responsibility shared by everyone at DOE, and I am confident that together, we can transform and strengthen DOE's enterprise cybersecurity posture and the posture of the U.S. energy sector to fulfill our diverse and vital missions on behalf of the American people.

David M. Turk
Deputy Secretary of Energy

Message from the Chief Information Officer

The March 2023 *National Cybersecurity Strategy* outlines a new vision for cybersecurity rooted in collaboration and accountability. In recognition of the priorities noted in the national strategy, the OCIO has developed this *DOE Cybersecurity Strategy* to define an integrated approach to reduce cybersecurity risks to the Department. This strategy also outlines how DOE will provide support to the U.S. energy sector by engaging in a range of high-impact activities to identify, deter, detect, and respond to threats against our critical assets.

DOE has a unique set of missions, spanning key Administration priorities including energy and nuclear security, modernizing the grid, promoting scientific research and discovery, cleaning up the Nation's environmental legacy, and combating climate change. This broad set of missions, combined with DOE's federated structure, presents unique cybersecurity challenges which requires an agile, risk-based approach to improve the security of IT and OT systems while enabling our missions.

This *DOE Cybersecurity Strategy* outlines an approach that will manage transformational change and achieve desired outcomes while addressing the challenges associated with an increasingly complex cyber threat landscape. Successful implementation will require transparent, inclusive, and collaborative governance processes with continued collaboration across Departmental Elements (DEs), Program Offices, Sites, Plants, and National Laboratories. Moving forward, we must employ a "collective defense" approach to cybersecurity, not only working with each other, but also across the Federal Government, private sector, and with allies and partners around the world to share best practices and leverage lessons learned.

Unfortunately, we do not have to look far to see the impact bad actors can have on our lives – ransomware attacks on healthcare facilities, oil pipelines, rail systems, and other areas of critical infrastructure; countless records and personal information stolen and used for criminal purposes – and many more examples that affect DOE's mission as well as our day to day lives. Worldwide cybersecurity incidents demonstrate how urgent and important this work really is. Our IT and OT infrastructure enables much of the vital work we do here in the Department, and we must take steps to ensure its defensibility and resiliency.

DOE's cybersecurity program must be flexible and adapt to emerging events and requirements. Even as I am writing this, new attacks are occurring, and new guidance and requirements are being issued from the Administration. This *DOE Cybersecurity Strategy* is designed to help us meet those evolving threats and vulnerabilities that we face today and will face in the future.

Ann Dunkin, P.E.
Chief Information Officer

Message from the Director, Cybersecurity, Energy Security, and Emergency Response

The world is increasingly interconnected and digitized and the U.S. energy sector is no exception. Cybersecurity is a necessity, and the Biden-Harris Administration has, appropriately, prioritized the development and implementation of cybersecurity strategies that will advance our overall security. The *DOE Cybersecurity Strategy* is the unifying document that defines how DOE will work internally to secure our own assets, information, and technology, and how we will work with the energy sector to protect and secure America's critical energy infrastructure.

The threats we face are significant and they are evolving. Sophisticated cyber criminals and groups take great interest in targeting our energy sector. With that in mind, DOE has a unique and important role to play, leading the effort to advance cybersecurity across the sector through collaboration with utilities and companies that own and operate so much of our infrastructure, by working with state and local officials to prioritize cybersecurity guidance for utilities, and by conducting research and development work with the National Laboratories, private sector, academia, and others.

The *DOE Cybersecurity Strategy* provides the vision necessary to secure our diverse energy sector. To implement the five pillars of this strategy we will need to innovate and collaborate, leaning on new approaches such as the Energy Threat Analysis Center, currently in its pilot phase, to enhance our ability to detect and mitigate cyber threats in close partnership with industry leaders. We'll also need to continue to prioritize workforce development through programs such as the CyberForce Competition and the OT Defender Fellowship.

From morning to night, Americans count on the reliable flow of energy via power lines, pipelines, and other types of infrastructure. As we move toward a clean energy economy, the future of energy generation, transmission, distribution, and use in the U.S. will be more digitized, interconnected, and complex. This new connectivity enables the energy sector to become more resilient, safe, and efficient, but it also introduces cybersecurity challenges. This is precisely why DOE is leading the charge to build in cybersecurity as we design the energy sector of the future, as outlined in the *National Cyber-Informed Engineering Strategy*. We're partnering across the Department to include cybersecurity in next generation energy technologies, electric vehicle infrastructure, and much more.

To meet the moment, we need to be both agile and steadfast in our approach to cybersecurity. The realization of the tenets of this strategy will help us to achieve our vision of a secure, reliable, and resilient energy sector for the American people.

Puesh Kumar

Puesh M. Kumar
Director, Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Message from the Chief Information Security Officer

Today's rapidly evolving cyber threat landscape presents unprecedented opportunities and challenges. As noted in the *National Cybersecurity Strategy* released in March 2023, digital technologies have shaped innovation and fostered change, advancing America's interconnectedness and prosperity. Cyber-attacks are evolving in complexity due to advanced technologies and we face increased persistent threats. We must be proactive in defending and securing the digital ecosystem and cyberspace.

Cybersecurity at the Department of Energy is an enterprise-wide responsibility, and it is critical to the success of the Department's varied missions of maintaining the Nation's nuclear deterrent, reducing the threat of nuclear proliferation, overseeing the Nation's energy supply, and managing the science and technology powerhouse of the 17 National Laboratories.

This uniquely broad and diverse mission set requires a federated model for oversight and management of all functions, including cybersecurity, across the enterprise. The *DOE Cybersecurity Strategy* aims to harmonize cybersecurity goals and initiatives across these various missions and foster a robust security culture.

Achieving a safe, secure, and resilient cyber environment requires DOE to take a risk-based approach through cost-effective investments to reduce cyber risk. In alignment with federal mandates, including Executive Order 14028, *Improving the Nation's Cybersecurity,* and the subsequent Office of Management and Budget (OMB) Memoranda, we recognize the need for increasing transparency between the government and private sector, as well as driving security through transformative initiatives such as Continuous Diagnostics and Mitigation, Endpoint Detection and Response, Ongoing System Authorization, Federal Information Technology Acquisition Reform Act (FITARA) Implementation, and Enterprise Network Monitoring.

Our goal is to be exemplary stewards of taxpayer dollars and continually improve provision of IT services and strengthen the Department's cybersecurity posture to enable our partners to perform the Department's mission through effective, efficient, and innovative management.

Paul Selby

Paul Selby
Chief Information Security Officer

Executive Summary

The DOE *Cybersecurity Strategy* is a plan for an effective, collaborative, enterprise-wide cybersecurity posture and defense. Given the Department's unique structure and mission, this strategy leverages diverse perspectives and experience from across the DOE enterprise, establishing a common understanding and a culture of collaboration and accountability. OCIO and CESER led the development of this strategy in collaboration with all relevant DEs, Program Offices, Sites, Plants, and National Laboratories. This strategy will be used to harmonize and prioritize DOE cybersecurity planning, programming, budgeting, training, and execution activities.

The increasing reliance on secure technology to achieve the Department's missions is our guiding light. Each of Energy's missions, which range from nuclear security, open science research, and clean energy development and deployment, to environmental management and operational enterprise functions, require safe, secure, and resilient technology and the cybersecurity solutions to ensure their operational success. DOE must continue to leverage its broad expertise and capabilities across the Department to strategically manage cybersecurity risks and ensure a secure, resilient, and defensible infrastructure for both the enterprise and the energy sector.

As such, we have identified five distinct strategic pillars to overcome some of our greatest challenges, fill key gaps, and accelerate the strengthening of DOE's cybersecurity posture. Within those five strategic pillars, this DOE *Cybersecurity Strategy* identifies specific goals and objectives, which DOE will pursue over the coming years to carry out its mandated cybersecurity responsibilities and address the evolving Departmental and energy sector cybersecurity needs. While Pillars 1-4 are more inward facing, Pillar 5 acknowledges not only DOE's own critical infrastructure assets, but also its relationship with the United States' energy sector as the Sector Risk Management Agency as well as its intersection with other critical infrastructure sectors.

Pillar 1, Understand the Risk: Understanding cybersecurity risks to the DOE enterprise by identifying threats, critical systems and their interdependencies and vulnerabilities, and estimating the likelihood and potential impact of cybersecurity incidents. Sound understanding of the overarching risk is required to effectively allocate resources, prioritize efforts, and develop an effective mitigation strategy.

Pillar 2, Mitigate Risk: Mitigating cybersecurity risks by applying zero trust cybersecurity principles and enhancing vulnerability management. Such protective efforts seek to reduce organizational and systemic risk of unintentional or malicious cyber activities and empower leadership to make informed risk-based decisions, improving the Department's overall cybersecurity posture.

Pillar 3, Enable Mission Resilience: Enabling mission resilience through enhanced governance and collaborative activities to make the Department's overall ecosystem more defensible. Aligning internal and external cybersecurity efforts will drive innovations that will help shift the advantage away from malicious actors toward those defending our systems and network.

Pillar 4, Develop the Cyber Workforce: Developing the workforce by improving cybersecurity awareness and capability. To protect networks and critical infrastructure, the Department must be armed with the right resources, people, and tools, including building and cultivating the workforce to effectively defend, deter, and protect our critical assets from threats.

Pillar 5, Protect Critical Energy Infrastructure: Protecting critical energy infrastructure by ensuring cyber resilience for assets, systems, and networks that provide functions necessary for execution of the broad DOE mission. This includes partnering with key stakeholders, such as other sector-specific agencies and the private sector, to drive improved cybersecurity by promoting the development and adoption of best practices.

While this strategy outlines activities specifically for DOE, the Department looks forward to conducting these efforts in partnership with the United States energy sector, and federal and non-federal partners throughout the nation and world. Through this strategy and the associated tasks, DOE will improve its posture and protect its systems, information, infrastructure, and the U.S. energy sector from the ever-evolving cybersecurity threats.

Introduction

The Threat

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten both the public and private sectors, and ultimately the security and privacy of the American people. Given the threats targeting the DOE complex, DEs, Program Offices, Sites, Plants, and National Laboratories should assume that networks and systems have been compromised by both known and unknown malicious actors seeking to exfiltrate our data and exploit the Department's users.

Malicious cyber activity has evolved from nuisance to damaging attacks against critical infrastructure, ransomware attacks, espionage, and theft of intellectual property. State-sponsored attacks from various nation states are aggressively using advanced cyber capabilities to carry out malicious activities and cause physical effects and are attempting to undermine our democracy. Historically, non-state actors and organized cyber criminals have successfully used ransomware to disrupt critical services and businesses across the international community, from energy pipelines and food supplies to educational and medical institutions. The Dark Web amplifies this problem by simplifying the sale of illicit goods and services, including malware and malicious cyber tools. Cryptocurrency also presents challenges to countering money laundering and the work of law enforcement. The rapid growth of generative artificial intelligence (AI) domestically and abroad is a potential accelerant of risk.

The proliferation of technology, including high performance computing, OT, large datasets, and integration of tens of billions of devices connected to the Internet, continuously creates new cybersecurity challenges, and leads to significant national security risks. Next-generation interconnectivity is collapsing the boundary between the digital and physical worlds and exposing some of our most essential systems to disruption. Our factories, power grids, nuclear plants, and water treatment facilities are among other essential infrastructure which are increasingly shedding old analog control systems in favor of digital OT. Advanced wireless technologies, Internet of Things (IoT), and space-based assets—including those enabling positioning, navigation, and timing for civilian and military uses, environmental and weather monitoring, and everyday Internet-based activities from banking to telemedicine—will accelerate this trend, moving many of our essential systems online and making cyberattacks inherently more destructive and impactful to our daily lives.

Supporting the Energy Mission

DOE is a large, diverse, and federated organization with an extremely broad mission set that requires numerous unique IT, OT, and cybersecurity solutions. This unique set of missions includes but is not limited to securing leadership in energy technologies, safeguarding our nuclear stockpile, cleaning up our environmental legacy, and maintaining vibrant efforts in science and technology as a cornerstone of economic prosperity. All DEs, Program Offices, Sites, Plants, and National Laboratories manage cybersecurity programs supporting DOE's missions, resulting in reliance on a Unity of Effort to ensure resilience across the DOE enterprise and business functions.

Departmental leadership integrates cybersecurity policies and operations throughout its myriad and vitally important operations. This includes weaving security into every aspect of operations, from leveraging actionable threat intelligence, addressing our environmental legacy, managing the science and technology powerhouse of the 17 National Laboratories, leading the transition to a clean energy future, and enhancing nuclear security to collaborating with the private sector, and State, Local, Tribal & Territorial (SLTT) partners to improve sector security. Collectively, we need to build a strong security posture; there can be no weak link.

These efforts rely on the guidance and leadership of the OCIO to develop and maintain information management security and technology policies and governance processes; lead and report on the Department's overall cybersecurity and technology portfolio risk posture to procure resources needed to support strategic direction, risk remediations, operational visibility, and coordinated incident response; train and enhance a cybersecurity and technology workforce; and foster interagency and cross-sector communications and partnerships.

This *DOE Cybersecurity Strategy* aligns with the March 2023 *National Cybersecurity Strategy* and represents a holistic approach to cybersecurity, which is a challenge given the landscape of the Department's diverse missions, each having its own unique risk profile. Accordingly, sound cybersecurity hygiene requires a collaborative approach. Factoring in the numerous and varied perspectives and experiences across the entire enterprise is essential to this strategy's success. Collaborative engagement will continue to be substantively formed around encouraging and receiving input, identifying and addressing issues, and proceeding with informed risk management-derived solutions that are conducive to mission success. There will continue to be ongoing integration, coordination, and partnering across all DEs, Program Offices, Sites, Plants, and National Laboratories to maximize this Unity of Effort across the DOE enterprise.

Our Vision

Using a Unity of Effort approach, DOE will leverage its broad expertise and capabilities across the Department to strategically manage cybersecurity risks and ensure a secure, resilient, and defensible enterprise and critical energy infrastructure. This is our North Star.

Our Approach

Applying a Unity of Effort approach requires a federated model for oversight and management of all functions, including cybersecurity and risk management, given DOE's uniquely broad missions. The federated model enables DEs, Program Offices, Sites, Plants, and National Laboratories to operate with significant independence to execute their missions while adhering to Department standards. At the same time, establishing an enterprise-wide cybersecurity strategy and risk management program requires aggregation across all organizations, functions, and missions.

DOE is taking this risk-based approach to cybersecurity across its federated enterprise to enable and advance the Department's missions through IT, OT, and cybersecurity policy, standards, and services. This approach addresses threats and vulnerabilities by setting performance goals and expectations while working collaboratively to modernize DOE cyber defenses and continuously adapting to an evolving threat environment. The Department must also work with other government agencies, industry, and our allies to build a defensible, resilient, and value-aligned digital ecosystem.

DOE cybersecurity policy and strategy development and implementation will be guided by cross-enterprise planning on cybersecurity, cyber preparedness, and resilience. Leveraging existing national guidance and a framework that considers the Department's and Nation's existing security posture, this strategy encourages the continued collaborative pursuit of a secure, resilient, and connected digital ecosystem that is aligned with our values and mission requirements.

Guiding Principles

DOE will advance its missions and accomplish its cybersecurity goals by aligning Departmental cybersecurity activities in accordance with the following guiding principles:

1. Risk prioritization. DOE will prioritize efforts to focus on systemic risks and the greatest cybersecurity threats and vulnerabilities to the DOE enterprise. This includes modifying cybersecurity priorities based on a sound risk management calculus that factors in the latest intelligence and real-world incidents and is informed by enterprise-wide lessons learned.

2. Cost-effectiveness. Cyberspace is highly complex. DOE efforts to increase cybersecurity will be continuously evaluated and reprioritized to ensure the best results for investments made.

3. Innovation and agility. Although the proliferation of technology leads to new risks, it also provides an opportunity for innovation. DOE, through its National Laboratories, will lead national efforts for research, development, and deployment of cutting-edge cybersecurity capabilities and remain agile in its efforts to keep up with evolving threats and technologies.

4. Collaboration. Through unity of effort, we will collaborate within the Department, across the Federal Government, with industry, and internationally, to share best practices and leverage lessons learned with a collective defense mindset.

5. National values. DOE will uphold privacy, civil rights, and civil liberties in accordance with applicable law and policy.

PILLAR 1

Understand the Risk

PILLAR 2

Mitigate Risk

PILLAR 3

Enable Mission Resilience

PILLAR 4

Develop the Cyber Workforce

PILLAR 5

Protect Critical Energy Infrastructure

PILLAR 1: Understand the Risk

DOE must understand the evolving global cybersecurity landscape and have insight into the threats to and the vulnerabilities of enterprise assets. This will enable the Department to effectively allocate resources and prioritize efforts to address threats, mitigate vulnerabilities, and understand cybersecurity consequences across the Department's wide array of missions.

- **Goal 1.1: Increase Threat Awareness.** DOE will increase awareness of trends in persistent and emerging threats, vulnerabilities, interdependencies, and potential consequences to enterprise cybersecurity to provide systems owners and Authorizing Officials a better understanding of the current threat landscape and potential mitigations.

  Objectives:
  - *Objective 1.1.1:* Increase sharing of actionable threat intelligence data within the Department, with external agencies, and other key stakeholders, as feasible, to ensure that system owners and Authorizing Officials are presented sufficient information to make informed, data-driven, and risk-based decisions.
  - *Objective 1.1.2:* Ensure that deployed cybersecurity tools can appropriately leverage threat intelligence.
  - *Objective 1.1.3:* Identify gaps in analytics capabilities for threat recognition as well as risk management efforts, and partner with key stakeholders to address these gaps.
  - *Objective 1.1.4:* Assess potential impacts of emerging or disruptive threats and technologies to support risk assessment and mitigation.

- **Goal 1.2: Increase Transparency in Vulnerability Reporting and Management**. DOE will apply a more rigorous approach to vulnerability management and reporting by incorporating information sharing, lessons learned, and best practices to understand applicability and estimate risk.

  Objectives:
  - *Objective 1.2.1:* Enumerate known vulnerabilities through timely updates to the Risk Register, including defining how to protect and monitor the systems they impact, and how to respond and recover from a cybersecurity incident.

- *Objective 1.2.2:* Increase participation in and transparency of the development, implementation, and close-out of Plans of Action and Milestones (POA&Ms) related to known vulnerabilities to enhance enterprise-wide risk management.
- *Objective 1.2.3:* Increase participation in DOE's Vulnerability Disclosure Program (VDP), use of penetration testing, and incident reporting to improve visibility and enable the enterprise to reduce risk and remediate vulnerabilities with expediency.

➢ **Goal 1.3: Increase Enterprise-wide Visibility and Accountability.** DOE will strive to maintain full visibility and accountability for all IT and OT systems to ensure they are known and managed within authorized environments.

Objectives:

- *Objective 1.3.1*: Establish OT inventory baselines to promote risk assessment on par with that of IT systems.
- *Objective 1.3.2*: Fully deploy the Cybersecurity and Infrastructure Security Agency's (CISA) Continuous Diagnostics and Mitigation (CDM) Program, to include full implementation of CISA's Binding Operational Directive (BOD) 23-01: *"Improving Asset Visibility and Vulnerability Detection on Federal Networks"* requirements, to enable continuous and comprehensive asset visibility and vulnerability enumeration in OT and IT environments.
- *Objective 1.3.3:* Update guidance to ensure that all required IT and OT systems are authorized by federal officials through an Authority to Operate (ATO) with timely, consistent, and transparent ATO execution, including selection and assessment of all relevant security controls.

➢ **Goal 1.4: Share Key Cyber Findings with System Owners and Authorizing Officials.** Leverage information sharing, including cybersecurity scorecards, across the enterprise to strengthen the cybersecurity posture of the Department and facilitate prioritization of investments.

Objectives:

- *Objective 1.4.1:* Enhance information sharing among Supply Chain Risk Management (SCRM) programs by building on the Center of Excellence Model to improve coordination and information sharing on technologies/vendors that have been assessed and/or authorized for use throughout the Department.
- *Objective 1.4.2:* Utilize data call responses, Enterprise Assessments, and Inspector General and General Accounting Office Audits to identify areas of weakness, excellence, and opportunities for targeted resource investment.
- *Objective 1.4.3:* Explore platform solutions where this information can be stored and easily shared and accessed by all stakeholders.

PILLAR 2: Mitigate Risk

DOE will prioritize the mitigation of risk based on likelihood and impact on DOE missions, processes, and employees. DOE must continually improve and validate its cybersecurity posture to address evolving threats.

- **Goal 2.1: Accelerate Implementation of a Zero Trust Architecture (ZTA).** DOE will build an architecture that uses strong multi-factor authentication (MFA), micro-segmentation, advanced encryption, endpoint security, analytics, and robust auditing, among other capabilities, to fortify devices, networks, data, applications, and services to deliver cybersecurity resiliency, consistent with the goals of the OMB M-22-09, "*Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.*"

  Objectives:

  - *Objective 2.1.1*: Implement MFA to the greatest extent possible or provide compensating security controls.
  - *Objective 2.1.2*: Implement encryption of data at rest, in use, and in transit to the greatest extent possible, and stand up an encryption working group to develop a crypto-agility roadmap for the transition to post-quantum cryptography.
  - *Objective 2.1.3:* Leverage knowledge gained from Zero Trust Maturity Assessments to apply best practices and strive to scale lessons learned and pilots into shared solutions across the enterprise when and where feasible.
  - *Objective 2.1.4***:** Fully deploy Endpoint Detection and Response (EDR) tools across the enterprise to detect and respond to incidents more readily, consistent with OMB M-22-01, "*Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems Through Endpoint Detection and Response.*"

- **Goal 2.2: Address Known Vulnerabilities.** DOE will apply a risk-based approach to reduce exposure by addressing known vulnerabilities and risks and prioritizing those that could have a major impact on the Department's mission.

Objectives:

- *Objective 2.2.1***:** Improve investigative and remediation capabilities by implementing event logging maturity capabilities outlined in OMB M-21-31, "*Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*," to enable more effective and resilient defense of DOE information systems.
- *Objective 2.2.2:* Rapidly and broadly alert anomalous activities within networks to help deter, detect, and mitigate both internal and external threats to the Department.
- *Objective 2.2.3:* Identify legacy systems and applications, their associated operational and cybersecurity risks, potential upgrade and mitigation costs, and priority for their modernization to reduce overall enterprise risk and technical debt.
- *Objective 2.2.4***:** Improve software supply chain security by identifying and enumerating all software, with prioritization of critical software, within the DOE environment to protect against exploitation when a new software vulnerability is announced, consistent with OMB M-22-18, "*Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*."

- **Goal 2.3: Optimize Use of Cloud Computing Solutions to Expand Defensive Cybersecurity Capabilities.** DOE will take advantage of cloud security services to monitor access to sensitive data and realize the security benefits of cloud-based infrastructure.

Objectives:

- *Objective 2.3.1*: Evaluate and update cloud architectural frameworks and maturity assessments to leverage lessons learned and best practices with clear, actionable recommendations to improve operations where applicable**.**
- *Objective 2.3.2:* Assess cloud business cases and identify opportunities for cost-effective shared services and enterprise agreements that empower secure user experiences.
- *Objective 2.3.3:* Use analytics to understand and optimize the Total Cost of Ownership of cloud infrastructure.

- **Goal 2.4: Validate Outcomes.** DOE will analyze mitigating security controls and their deployed functionality with a comprehensive approach to validate expected cybersecurity behaviors and outcomes to gain confidence in the security of information systems and mitigation capabilities.

Objectives:

- *Objective 2.4.1:* Identify existing programmatic capabilities and gaps for testing and validation, including static application testing.
- *Objective 2.4.2:* Capture and document lessons learned to identify deviations, measures of success, and remediation of potential weaknesses.
- *Objective 2.4.3:* Promote strong cyber hygiene and emergency preparedness by testing workforce abilities and behaviors against expectations.
- *Objective 2.4.4*: Conduct exercises that stress cyber and emergency management procedures to validate expected outcomes.

PILLAR 3: Enable Mission Resilience

DOE will align efforts across the enterprise to enable the success of its missions through streamlined cybersecurity risk management. This will be accomplished through supporting policy and operational efforts that make the entire enterprise more secure and resilient. Such efforts help shift the advantage away from malicious cyber actors toward those protecting our critical mission assets.

- **Goal 3.1: Enhance Governance; Update Policies and Guidance.** DOE will improve cybersecurity risk management outcomes by supporting policy, governance, and operational efforts that make the entire ecosystem more secure and resilient.

  Objectives:
  - *Objective 3.1.1:* Assess and update governance models, DOE Directives, DOE Policies, and other guidance to ensure updated laws, regulations, and government-wide policies are incorporated.
  - *Objective 3.1.2*: Encourage secure by design practices by embedding cybersecurity in systems engineering and acquisition processes.
  - *Objective 3.1.3:* Standardize reference architectures, where applicable.
  - *Objective 3.1.4*: Ensure cybersecurity program plans are updated and maintained as part of the maturation of security governance across the enterprise.

- **Goal 3.2: Ease Burdens.** DOE will seek opportunities to reduce redundancies, streamline processes, and leverage economies of scale to provide for more efficient use of resources**.**

  Objectives:
  - *Objective 3.2.1*: Identify opportunities for economy at scale including additional enterprise licensing.

- *Objective 3.2.2:* Evaluate automation solutions for data calls to reduce redundancies.
- *Objective 3.2.3:* Consolidate oversight and accountability requirements, where feasible.
- *Objective 3.2.4:* Participate in federal cyber regulatory harmonization efforts to reduce dual regulatory compliance standards that exist for many of our DEs/sites.

➢ **Goal 3.3: Improve Cyber Agility.** DOE will improve its ability to continuously adapt to emerging and disruptive threats.

Objectives:

- *Objective 3.3.1*: Develop guidance to counter the cyber threats of emerging technologies including, but not limited to, Quantum Computing and AI.
- *Objective 3.3.2:* Leverage the National Laboratories to advance research, development, and deployment of technologies, tools, and techniques to reduce risks to federal systems and our critical energy infrastructure posed by emerging cybersecurity threats.
- *Objective 3.3.3:* Identify, develop, transition, and deploy technology innovation that improves our cybersecurity posture.
- *Objective 3.3.4:* Update the DOE Incident and Vulnerability Response Playbook based on CISA Guidance to evolve our ability to identify, coordinate, remediate, recover, and track successful mitigations from incidents and vulnerabilities through more standardized practices.
- *Objective 3.3.5:* Leverage CISA's Security Operations Center (SOC) Maturity Model to assess and improve threat monitoring, detection and incident response, threat intelligence, and cybersecurity investigations.

➢ **Goal 3.4: Expand Collaboration.** DOE will enhance its public, private, interagency, and international partnerships to advance shared goals and promote the sharing of best practices and lessons learned.

Objectives:

- *Objective 3.4.1:* Develop and maintain relationships with key international partners that advance our cooperation on sharing of cybersecurity best practices, information, expertise, and technical assistance.
- *Objective 3.4.2:* Establish an enterprise-wide Cybersecurity Center of Excellence to serve as a collective hub for training, guidance, and technical assistance.
- *Objective 3.4.3*: Expand collaboration with the interagency, private sector, and academia to promote a collective defense approach to cybersecurity.
- *Objective 3.4.4:* Share information on known vulnerabilities, mitigations, and trusted and unverified suppliers with industry, the interagency, and international partners on a timely basis, when appropriate.
- *Objective 3.4.5:* Support the strengthening of cyber response processes across the U.S. Government and the Department by providing technical assistance for emerging crisis incident requirements.

PILLAR 4: Develop the Cyber Workforce

DOE will address critical cybersecurity talent shortages through active and thoughtful recruitment, retention, and training of cybersecurity personnel. DOE will further enhance its culture of inclusivity and optimize the employee experience with ongoing opportunities for professional development to strengthen the existing cyber workforce and grow the supply of qualified new talent.

- **Goal 4.1: Fully Characterize and Understand the DOE Cyber Workforce.** DOE will improve its recruitment, retention, and career development processes to facilitate the hiring of a qualified, diverse workforce, while also ensuring exceptional recruitment and hiring experiences for applicants and hiring managers.

  Objectives:

  - *Objective 4.1.1:* Collect department-wide cyber workforce information including: funded and unfunded cyber vacancies, hiring projections, turnover rates and drivers, retirement eligibility, work role distribution, grade level distribution, cyber certifications, and current skills via assessment to better understand the size, disposition, composition, and developmental needs of DOE's federal cyber workforce.
  - *Objective 4.1.2*: Regularly assess and update the Department's cyber workforce Work Roles of Critical Need (WRCN) to help DOE shape and direct its recruitment, development, and retention initiatives.
  - *Objective 4.1.3:* Leverage future OPM training to develop a cadre of DOE Human Resource (HR) specialists knowledgeable in cyber talent management and succession planning to better support the Department's cyber recruitment, development, and retention initiatives.

- **Goal 4.2: Recruit, Grow, and Retain a Qualified, Diverse Cyber Talent Pool.** DOE must articulate the appealing benefits of its mission and provide more robust on-ramps through opportunities at every stage of career development to attract and retain a qualified and diverse cyber workforce.

  Objectives:

  - *Objective 4.2.1:* Promote entry-level and career ladder positions to establish a talent pipeline and aid in succession planning.
  - *Objective 4.2.2:* Create job postings that clearly focus on need-to-have skills based on National Initiative for Cybersecurity Education (NICE) work roles and expand the use of shared hiring actions focused on DOE's WRCNs to broaden the talent pool and facilitate faster, higher quality hires.
  - *Objective 4.2.3:* Partner with professional programs and organizations working with under-represented or disadvantaged groups to offer nontraditional internship and apprenticeship opportunities for cybersecurity-focused 501(c)(3) organizations and promote DOE's various cyber internship programs, such as the Omni Alliance Internship Program, to expand the talent pool into historically marginalized populations.
  - *Objective 4.2.4*: Implement the Cybersecurity Retention Incentive Program piloted in FY23 as an enterprise-wide approach to retain targeted WRCNs and continue to review program for effectiveness.

- **Goal 4.3: Promote Professional Development Through Training and Awareness.** DOE will develop model cyber career pathways that present attractive careers within and across the Department to provide cybersecurity professionals the necessary specialized skills and continuous development to stay ahead of the rapidly evolving threat environment.

  Objectives:

  - *Objective 4.3.1:* Develop a cyber training catalog and learning and career development/succession roadmaps for relevant work-role related Departmental and federal resources as well as training and certifications from external and commercial vendors.
  - *Objective 4.3.2:* Develop and pilot a Cyber Workforce Development Program focused on the Department's WRCN that assesses cyber practitioners' skill level and provides DE-funded training recommendations based on assessment performance.
  - *Objective 4.3.3:* Coordinate with management to leverage the NICE Framework, CISA National Initiative for Cybersecurity Careers and Studies (NICCS) Cyber Careers Pathway Tool, and federal cyber workforce development and education programs to incorporate skills-based cyber education and training into Individual Development Plans.
  - *Objective 4.3.4:* Expand skills-based training initiatives into adjacent disciplines (e.g., OT, AI, and data analytics) including procuring enterprise licensing agreements for training providers.

PILLAR 5: Protect Critical Energy Infrastructure

Ensuring cyber resilience for the Nation's critical infrastructure is a top priority for DOE in response to the growing landscape of new threats, technologies, and trends. Defending critical infrastructure systems, both those owned by DOE, and those within the energy sector, is vital to our national security, public safety, and economic prosperity. DOE must drive improved cybersecurity for the energy sector in its role as the Sector Risk Management Agency. DOE must also be a good partner to all critical infrastructure sectors that DOE elements intersect with to carry out their broad missions.

- **Goal 5.1**: **Increase Cyber Visibility and Defense of Existing Critical Infrastructure Systems and Networks.** The Department will enhance the development of technologies and systems that increase the ability to detect and analyze emerging cyber threats targeting our critical infrastructure to proactively protect, defend, and respond to cyberattacks.

  Objectives:

  - *Objective 5.1.1*: Promote adoption of ZTA, improve critical infrastructure network visibility, and remediate identified vulnerabilities to support improved critical infrastructure resiliency.
  - *Objective 5.1.2*: Characterize and prioritize risks in the energy sector through ongoing rigorous analysis in coordination with U.S. Government and sector partners, including the use of operational collaboration programs such as the Energy Threat Analysis Center.
  - *Objective 5.1.3*: Implement and test cyber incident response and recovery plans for critical infrastructure control systems to enable more efficient and effective response, disruption, and mitigations of cyberattacks, and support efforts to revise the National Cyber Incident Response Plan to highlight the Department's unique capabilities and resources.
  - *Objective 5.1.4:* Refine and clarify functional relationships across the Department to identify baseline data and systems requirements to further advance security and resilience.
  - *Objective 5.1.5:* Enhance public-private collaboration opportunities through ongoing and new structures to identify, detect, and analyze emerging risks to critical infrastructure assets, systems, and networks.

- **Goal 5.2: Build Security into Future Critical Infrastructure.** The Department will advocate for the usage of and employ the use of secure by design and cyber resilience practices to better anticipate, withstand, operate through, recover from, and adapt to adverse conditions, stresses, attacks, or compromises.

  Objectives:
  - *Objective 5.2.1:* Lead public-private partnerships to inform energy sector security and resilience of all threats and hazards, including specific emphasis on cybersecurity from adversarial threats.
  - *Objective 5.2.2*: Partner with the energy sector and National Laboratories to operationalize the Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program to identify high priority OT components prevalent in the Nation's critical energy systems, test and share information about their vulnerabilities, and inform improvements in component design and manufacturing to prevent exploitation.
  - *Objective 5.2.3:* Leverage key lessons learned from DOE and industry cyber supply chain risk management efforts to identify and address cyber supply chain risks and develop a supply chain risk management strategy for the U.S. energy sector that outlines policies, tools, technologies, and other measures to tackle cyber supply chain threats.
  - *Objective 5.2.4:* Implement the National Cyber-Informed Engineering (CIE) Strategy to protect energy and other critical infrastructure by building security into the earliest stages of device or system design and development.
  - *Objective 5.2.5:* Conduct research, development, and demonstration projects in partnership with industry, academia, and National Laboratories to address cybersecurity in next generation energy systems to increase security that will identify, protect, prevent, mitigate, and respond to current and future threats to energy systems.

- **Goal 5.3: Enable Cyber Preparedness.** DOE will establish policies, processes, baseline principles, and training that advance physical protection and incident response, and promote cyber hygiene of control systems for critical infrastructure with an emphasis on energy sector control systems.

  Objectives:
  - *Objective 5.3.1:* Improve protections against physical intrusions to federal control system equipment and systems and limit unintentional access by applying robust physical security based on federal and other regulatory requirements and share best practices with industry stakeholders as practical.
  - *Objective 5.3.2:* Invest in U.S. Government, industry, and state capacity building activities such as tabletop exercises and critical infrastructure readiness exercises to enhance risk management, response to, and mitigation of cyber threats.
  - *Objective 5.3.3:* Utilize stakeholder groups such as the DOE OCIO Control Systems Working Group (CSWG) and industry groups such as the Electricity Subsector Coordinating Council to help guide and translate federal strategic priorities and requirements into actionable implementation guidance for DOE's ICS/OT system owners.
  - *Objective 5.3.4*: Provide threat intelligence analysis to the energy sector that includes context around significant tactics, techniques, and procedures being shared and what the Energy Sector can do to mitigate potential impacts.
  - *Objective 5.3.5*: Increase training, exercises, and workforce develop to the energy sector to strengthen its capabilities in OT cybersecurity.

Implementation

In collaboration with DEs, Program Offices, Sites, Plants, and National Laboratories, OCIO and CESER will develop a *Cybersecurity Strategy Implementation Plan* (*Plan*) to supplement this *DOE Cybersecurity Strategy* by providing the operational blueprint for maturing the Department's cybersecurity activities consistent with the principles and goals outlined in this strategy document. OCIO and CESER will annually assess the implementation of this strategy and provide a report to the Deputy Secretary. The report will include areas of success, opportunities for improvement, constraints impeding progress, and suggested adjustments to the strategy. The *Plan* will then be updated annually with consideration of the Department's budget formulation and execution processes. It is important that cybersecurity receives adequate resource allocations and focus commensurate with its priority status. Without appropriate resources, a cybersecurity incident could cause significant harm that can cascade exponentially, leading to mission failure and, as importantly, loss of stakeholder trust.

Conclusion

DOE will strive to improve its cybersecurity posture for the delivery of its essential missions and services. We will do so in a collaborative manner, within DOE, with other federal agencies, the private sector, and other stakeholders, across all our mission areas to ensure that cybersecurity risks are effectively managed, critical networks are protected, vulnerabilities are mitigated, and incident response is conducted in a timely way. Meeting the goals and objectives outlined in this strategy requires a unified, long-term approach across the Department. Aligning Departmental goals, activities, and resources will enhance DOE cybersecurity efforts moving forward. Through prioritizing requirements and taking a risk management-based approach to cybersecurity, the Department will establish a strong foundation for combating ever-increasing cybersecurity threats.