U.S. Department of Energy

CYBERSECURITY STRATEGY

2018-2020

U.S. Department of Energy
Cybersecurity Strategy 2018 - 2020

MESSAGE FROM THE DEPUTY SECRETARY

Advancing cybersecurity is a core priority for the Department of Energy (DOE). Our Department is approaching the cybersecurity challenge as an enterprise effort, incorporating assets and capabilities from across our programs and National Laboratories. This ***DOE Cybersecurity Strategy*** will focus attention on our critical cybersecurity mission of protecting our Federal systems and networks. This Strategy, in concert with the recently-published ***DOE Multiyear Plan for Energy Sector Cybersecurity***, is a significant step toward achieving better coordination of key cyber operations across the Department.

In my role as chair of the DOE Cyber Council, I have had the privilege of meeting and working with IT and cybersecurity policy and technical leaders across the Department to advance an enterprise-wide approach to cybersecurity. This Strategy and Implementation Plan reflects the outcome of our efforts and identifies the steps we will take to ensure that cyber resources are allocated across DOE as effectively as possible. It is a crucial roadmap for how to translate our cybersecurity priorities into action to protect the Department's most valuable assets.

This plan lays out a number of specific things we must do – or continue to do – in order to ensure the enterprise-wide success of our collective cybersecurity mission:

- Sharing cyber threat data in near-real time, as well as mitigating those threats by expediting and elevating the analysis of that data using U.S. intelligence assets.
- Developing common identity services to allow better collaboration and visibility.
- Partnering with fellow Federal agencies to identify and implement best practices.
- Fully implementing Continuous Diagnostics and Mitigation (CDM) tools across the enterprise to provide scalable, risk-based, cost-effective cybersecurity solutions.
- Enhancing DOE's Integrated Joint Cybersecurity Coordination Center (iJC3) to ensure enterprise visibility in real-time to stay a step ahead of our adversaries.
- Working to build a system that connects everyone at DOE in the cloud, while safeguarding internal communications and sensitive data.
- Implementing a cyber risk management framework to prioritize investments and improve our responses to rapidly evolving threats.
- Continuing to identify, investigate, and mitigate threats posed by individual and organized threat actors.
- Combating targeted phishing, denial of service attacks, and the introduction of malware into our systems.
- Continuing to leverage the work of our National Laboratories as they accelerate their development of innovative cybersecurity capabilities.

The priorities outlined in this document are essential to meeting the challenge of our shared cyber mission. Cybersecurity is a responsibility shared by everyone at DOE, and I am confident that together, we can transform and strengthen DOE's cyber posture across the enterprise in order to fulfill all of our diverse and vital missions on behalf of the American people.

I am pleased to endorse the Cybersecurity Strategy of the Department of Energy for 2018-2020.

Dan Brouillette
Deputy Secretary of Energy
June 2018

U.S. Department of Energy Cybersecurity Strategy 2018 - 2020

MESSAGE FROM THE CHIEF INFORMATION OFFICER

The U.S. Department of Energy Office of the Chief Information Officer has prepared this DOE Cybersecurity Strategy and Implementation Plan to improve the cybersecurity and resilience of the Department's networks and systems. It lays out an integrated strategy to reduce cyber risks to the Department and provide support to the U.S. energy sector by engaging in a range of high-impact activities in coordination with other DOE offices and the strategies, plans, and activities of the Federal Government. The Strategy will also support the energy sector by reinforcing the Department's Multiyear Plan for Energy Sector Cybersecurity. The Cybersecurity Strategy is aligned to the Multiyear Plan to reduce the risk of energy disruptions due to cyber incidents and describes how DOE will carry out its mandated cybersecurity responsibilities and address the Department's evolving cybersecurity needs.

Our Cybersecurity Strategy and Implementation Plan will manage transformational change, improve outcomes, and establish a sustainable cybersecurity future. This strategy is structured around:

- **Mission Alignment** – ensuring a direct line between the DOE Strategic Plan and the Cybersecurity Strategy;
- **Customer and Stakeholder Alignment** – Bringing value to both customers and stakeholders by strengthening collaboration with a brokerage posture;
- **Process Alignment** – Ensuring processes create value through analytics and business intelligence, to achieve sustainable levels of performance, execution, and innovation; and
- **Resource Management Alignment** – ensuring our workforce strategy helps to recruit, develop, and retain the talent we need to meet the needs of the DOE enterprise.

The DOE Cybersecurity Strategy addresses the challenges associated with an increasingly complex cyber landscape. Successful implementation of our strategy will require a transparent, inclusive, and collaborative governance process across DOE Staff Offices, Program Offices, National Laboratories, Power Marketing Administrations, Plants, and Sites. This Strategy will help to modernize DOE IT infrastructure to deliver effective services that will support smart, efficient cybersecurity and enhance DOE's cybersecurity risk management across the enterprise. Our network modernization initiatives will improve IT infrastructure, enhance cybersecurity, increase resiliency (including the expanded use of cloud services), scale capacity commensurate with demand to meet customers' needs, raise awareness, and promote best practices across the DOE enterprise. Our Cybersecurity Strategy and Implementation Plan will deliver high quality IT and cybersecurity, continuously improve our cybersecurity posture, help us make the transition from IT owner to IT broker, and excel as stewards of taxpayer dollars.

I am pleased to present the Cybersecurity Strategy of the Department of Energy for 2018-2020.

Max Everett
Chief Information officer
Department of Energy
June 2018

Contents

Executive Summary

The Department of Energy (DOE) leads the Federal Government's effort to ensure cybersecurity attacks do not have a catastrophic impact on the energy sector, as well as to ensure the cybersecurity and resilience of the DOE Enterprise infrastructure.

In furtherance of its mission, DOE is releasing this *Cybersecurity Strategy*, a plan for an effective, collaborative, enterprise-wide cybersecurity posture and defense. Given the Department's unique structure and mission, the plan leverages diverse perspectives and experience from across the Energy Enterprise, establishing a common understanding and a culture of accountability.

The Strategy identifies four crosscutting principles:

- "One Team, One Fight"
- Employment of risk management methodology
- Prioritized planning and resourcing
- Enterprise-wide collaboration

The Department will apply these principles across four *IT Strategy* goals:

- IT Goal 1. Deliver high-quality IT and cybersecurity solutions
- IT Goal 2. Continually improve cybersecurity posture
- IT Goal 3. Transition from IT owner to IT broker for better customer focus
- IT Goal 4. Excel as stewards of taxpayer dollars

Within those four goals, the *Cybersecurity Strategy* identifies seven objectives, with associated major tasks and activities, which DOE will pursue over the next three years to reduce the risk of cybersecurity incidents. The strategy describes how DOE will carry out its mandated cybersecurity responsibilities and address the evolving Departmental security needs.

The *Cybersecurity Strategy* also establishes the guiding principles and strategic approach needed to drive both near- and long-term priorities for DOE Enterprise and energy-sector cybersecurity. It aligns with related frameworks and strategies, including the National Institute of Standards and Technology (NIST)'s Cybersecurity Framework, and the President's Management Agenda. The strategy also furthers the implementation of several statutes and executive orders related to cybersecurity, including the Federal IT Acquisition Reform Act (FITARA), Federal Information Security Management Act (FISMA), and Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

Finally, the strategy will provide critical support to DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the office dedicated to cybersecurity and incident response activities for the energy sector.

While the strategy outlines activities specifically for DOE, the Department looks forward to conducting these efforts in close partnership with the energy industry and Federal and non-Federal partners throughout the nation. Through this strategy and the associated tasks, DOE will improve its posture and protect its systems, information, and infrastructure from the cybersecurity threat.

Introduction

Cybersecurity is critical to the success of the Department of Energy's varied missions from 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. Protecting these vital missions from the ever growing and complex cyber threats we face is crucial, and Secretary Perry has no higher priority.

This Department of Energy (Department or DOE) *Cybersecurity Strategy* (and associated *Implementation Plan* (collectively, *Cybersecurity Strategy*)) provides the roadmap for an effective, collaborative enterprise-wide cybersecurity defense. The *Cybersecurity Strategy* is rooted in risk management-based principles, which is to be codified in policy, resourced, and rapidly operationalized across the DOE enterprise with measurable metrics associated with each prioritized goal and task. In line with Deputy Secretary Brouillette's adage that, "We are one team, one fight," each Department component must be "all in," fully invested in enterprise-wide cybersecurity collaboration—there can be no weak links.

The *Cybersecurity Strategy* aligns with the President's 2017 *National Security Strategy*[1] , which calls for protection of both Federal and Energy sector assets and Congressional Direction provided in the FY 2018 Enacted Budget[2].

Given the vast scope and scale of cybersecurity threats — rapidly evolving in diverse form and function — set against the Department's operating structure, comprising 107 Departmental elements spread across over 30 states, the Department's Cybersecurity Program needs to be flexible and dynamic to ensure continued DOE mission success. Accordingly, this *Cybersecurity Strategy* is built on successful elements of DOE's enterprise-wide cybersecurity collaboration, strategic thinking, and tactical operations, and is calibrated to not "break mission." It also reflects the latest innovative approaches and best practices across the Federal Government and industry, and factors in feedback received from the Congress, the Government Accountability Office (GAO), and the Department's Office of Inspector General (OIG).

The Department's Chief Information Officer (CIO), partners with cybersecurity professionals and executives across the Department — leveraging their expertise, insight, and resources — to lead the Department's Cybersecurity Program on behalf of the Secretary in accordance with the *Federal Information Security Modernization Act of 2014* (FISMA), Executive Orders and Memoranda, National Institute of Standards and Technology (NIST) standards and practices (such as the *Framework for Improving Critical Infrastructure Cybersecurity* (*Cybersecurity Framework*)), Department of Homeland Security (DHS) Binding Operational Directives, and Department policies, to include DOE Order 205.1, *Cyber Security Program*.

Additionally, the *Cybersecurity Strategy* aligns to the recently released Department's *Multiyear Plan for Energy Sector Cybersecurity* to strengthen the cybersecurity and resilience of the nation's energy infrastructure, including DOE's own Power Marketing Administrations.

Cybersecurity Vision

Many missions working together as one efficient and effective enterprise to provide best-in-class security across the Department of Energy.

Cybersecurity Mission

Advance the Department's mission through the collaborative development and adoption of enterprise-wide cybersecurity policies matched by prioritized risk management-based implementation of cybersecurity defenses that enable outstanding customer operations while balancing risk, resource constraints and the need for innovation, and that are subject to clear and measurable performance goals for securing information resources and systems Department-wide.

[1] https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
[2] https://docs.house.gov/billsthisweek/20180319/DIV%20D%20EW%20SOM%20FY18-OMNI.OCR.pdf

Principles for Success

1. "One Team, One Fight"

The Secretary and Deputy Secretary recognize that malicious actors and nation-states are intent on preventing the Department from performing its mission. Accordingly, they have clearly and repeatedly enunciated that cybersecurity is a top priority for Department. Departmental leadership must integrate cybersecurity policies and operations throughout the Department's myriad and vitally important activities. There can be no weak links. To be successful, leadership must maintain its focus on the Departmental cybersecurity goal, which ultimately supports all of Departmental goals and Primary Mission Essential Functions / Mission Essential Functions.

2. Employment of Risk Management Methodology

Given limited resources, DOE must prioritize its cybersecurity requirements against a risk management filter. Cybersecurity threats will remain dynamic, and given their insidious nature, the Department must, likewise, be agile in evaluating and modifying its 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. In many instances, the office best-suited to analyze and appreciate risk will be at the component level. The Department must recognize the benefits of their vantage points and empower them to balance cybersecurity risk. They, likewise, must understand that, given the vast scope and scale of rapidly evolving cybersecurity threats in diverse form and function, the Department must constantly calibrate its cybersecurity defense-in-depth and defense-in-breadth posture.

3. Prioritized Planning and Resourcing

Cybersecurity must receive resource allocations and focus commensurate with its priority status. Department planning, budgeting, and execution without cybersecurity at the fore can, as history has revealed at the Department, at other agencies, and in the private sector, result in harm that can cascade exponentially, leading to mission failure and, as importantly, loss of stakeholder trust. Unplanned or emergency expenditures for cybersecurity will be factored into budget discussions. The Department, however, must be a responsible steward, correlating resource allocations to measurable metrics and process improvements based on observable results. For their part, leaders must be accountable for failing to prioritize cybersecurity hygiene and reporting on operational metrics. 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. This supports implementation of Executive Order (EO) 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which directs DOE and other Federal agencies to examine how Federal authorities and capabilities can support cyber risk management.

4. Enterprise-wide Collaboration

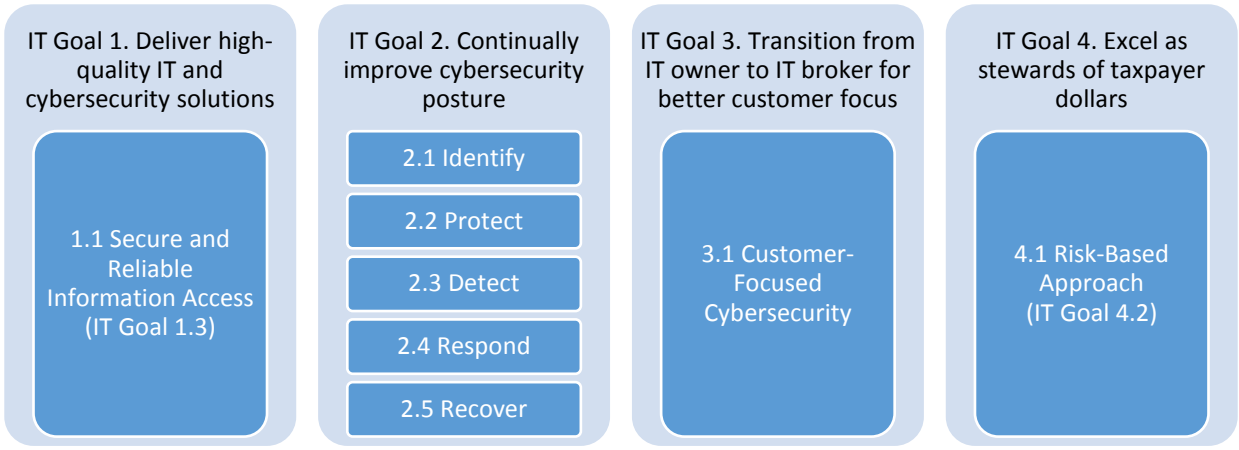
The Department needs a holistic approach to cybersecurity, which is a challenge given the Department's diversity, comprising sites, National Laboratories, and plants spread across over 30 states, each with unique missions and unique risk profiles. Accordingly, sound cybersecurity defense requires a collaborative and customer-focused approach—especially where mission requirements vary greatly, even within Departmental elements. Factoring in the numerous and varied perspectives and experiences Department-wide is essential to the success of the *Cybersecurity Strategy.* Key to customer engagement is soliciting customer input/feedback and determining and understanding customer requirements. Likewise, the value proposition for cybersecurity measures must be clear to customers. The collaborative engagement will be substantive, formed around encouraging and receiving input, identifying and timely addressing issues, and proceeding with informed risk management-derived solutions that are conducive to mission success. Informed and engaged *customers* are more likely to become invested *partners*. There will be ongoing integration, coordination and partnering across NNSA, Science, Energy and the other Departmental Elements to secure the enterprise as One Team, One Fight.

Departmental Alignment

The Department's newly formed CESER Office leads the Federal Government's effort, in concert with Energy sector owners and operators, to ensure cyber and physical attacks do not have a catastrophic impact on the Nation's Energy sector. Internally, the Secretary has charged the CIO with responsibility for enterprise-wide cybersecurity risk management per Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (2017) (E.O. 13800). The *Cybersecurity Strategy* is framed to respect operational boundaries, and, equally, to foster synergies between CESER and the OCIO.

Cybersecurity Strategic Objectives

Each goal of the DOE CIO's *IT Strategy* is matched to corresponding cybersecurity objectives supported by major tasks as described below. The objective for IT Goal #2 tracks each function of NIST's *Cybersecurity Framework*: Identify, Protect, Detect, Respond, and Recover.



GOAL 1 - DELIVER HIGH-QUALITY IT AND CYBERSECURITY SOLUTIONS

Objective 1.1 - SECURE and RELIABLE INFORMATION ACCESS

To achieve mission success, DOE's employees and stakeholders must have secure and reliable access to mission-essential systems, networks, and information resources.

MAJOR TASKS:

- Ensure the availability of and access to systems, networks, and information resources that enable DOE to perform the full lifecycle of its mission-essential functions.
- Provide service providers, customers, and stakeholders with timely and accurate information necessary for them to make informed risk management-based decisions.
- Ensure that Departmental High Value Assets (HVAs) are protected by cybersecurity and physical controls, as well as, adequately managed and resourced throughout their lifecycle.
- Strengthen the cybersecurity of corporate data and information resources data centers.
- Leverage new network paths and secure data transfer technologies to increase internal and external information flow across DOE sites and operating environments.
- Integrate Supply Chain Risk Management (SCRM) with mission-oriented, risk-based protections that support information technology-based services, external access, and collaboration.
- Provide enhanced role-based cybersecurity training requirements and programs to ensure that users are fully cognizant of their responsibilities for protection of the Department's information resources.

GOAL 2 - CONTINUALLY IMPROVE CYBERSECURITY POSTURE

Objective 2.1 IDENTIFY – *Enhance organizational capabilities to manage the cybersecurity risk.*

E.O. 13800 calls on the Secretary to implement risk management measures and ensure that cybersecurity risk management processes are aligned with strategic operational and budgetary planning processes. To normalize cybersecurity risk activities enterprise-wide, the Department is leveraging established guidelines, including the Cybersecurity Capability Maturity Model, Cybersecurity Evaluation Tool, and Electricity Subsector Cybersecurity Risk Management Process to provide common standards and reference points necessary to catalog enterprise-wide capabilities and assess cybersecurity risks. The Department's collaboratively developed enterprise-wide Data Taxonomy establishes the baseline for comprehensive and standardized cybersecurity metrics reporting.

The Cybersecurity strategy is aligned to the department's multiyear plan for energy sector cybersecurity which seeks to expand capabilities to monitor, analyze, and share OT threat indicators. Robust security requires monitoring and securing both enterprise IT environments and operational environments.

MAJOR TASKS:

- Develop policies that direct the establishment of cybersecurity hygiene through the use of automated tools, strengthening of internal controls, and standardization of processes and reporting to reduce the cost and management complexity of cybersecurity functions.
- Adopt standards and processes that facilitate and accelerate the secure integration of innovative IT solutions.
- Conduct assessments to ensure that integration of new IT hardware, software, and firmware meet cybersecurity standards (along with legal and regulatory requirements) to prior to integration into the Department's information ecosystem.
- Overseeing and analyzing assessments to make an overall assessment of the Department's risk posture.

Objective 2.2 PROTECT - *Develop and implement enterprise controls to reduce risk and increase resilience; promote enterprise cybersecurity awareness through workforce development and training.*

DOE continues to develop requirements and corresponding solutions to ensure the confidentiality, integrity, and availability of its information resources. It embraces standards and best-practices, regardless of origination, if they can lead to operating efficiencies, cost reduction, and quicker integration of innovative IT solutions. The Department is not averse to raising standards above thresholds set by *FISMA*, Information Sharing and Safeguarding (IS&S), and other Federal cybersecurity requirements where they can improve its provision of secure, reliable, and effective services to the Department and its stakeholders. The Department also is strengthening its accreditation standards to better safeguard its information resources and minimize the exposure from insider threats.

In particular, the Department is improving policies and controls hardening the DOE infrastructure and network environment by, among other things, increasing the use of strong authentication, controls on privileged access, audit assessments, and Identity, Credential, and Access Management (ICAM) processes. An enterprise-wide collaboration has led to a trusted framework and common identity infrastructure. The Department is deploying cybersecurity assets and tools, to include Continuous Diagnostics and Mitigation (CDM) across the enterprise, and is also assisting with the deployment of tools designed to harden the overall security of the Nation's Bulk Electric System.

Preparing, training, and equipping the Department's workforce — regardless of job function — is essential to mission success and protecting the Department's information resources. Universal cybersecurity awareness, behaviors, and skills improve the Department's ability to promptly identify, evaluate, and counteract threats, whether potential or actual. By investing in cybersecurity training, education, and awareness, the Department fosters a culture of cybersecurity that empowers its personnel—acting in accordance with cybersecurity policies, procedures, and practices — as force multipliers in the first-line defense against growing and persistent, pervasive cyber threats. According to the Deputy Secretary, cybersecurity "must be a mission that everyone at DOE owns—regardless of job title, position, and description."

To keep its workforce current on best-in-class security practices, the Department is enhancing its cybersecurity training and workforce development programs, including role-specific training and training on security policies and procedures, rules of behavior, and user awareness. The Department is actualizing cost savings by sharing common training resources with the Department of Defense.

MAJOR TASKS:

- Design and implement cybersecurity requirements, measures, and solutions that harden DOE's infrastructure and network environment, thereby increasing protection of its information resources.
- Execute a Department-wide approach to ICAM to control accessibility of Department information resources, systems, and facilities.
- Augment and support enhanced cybersecurity services at all Department sites.
- Provide relevant training, education, and awareness to all DOE employees regarding cybersecurity threats, risks, and impacts, thereby encouraging greater individual accountability and responsiveness.
- Develop a highly capable cybersecurity workforce through specialized, role-based training and development.
- Improve current cybersecurity training curriculum, to include human performance assessment programs.

Objective 2.3 DETECT - *Develop tools and processes to accelerate notification of cybersecurity threats.*

DOE employs best-in-class tools necessary to accelerate cyber threat detection, notification, and response across the enterprise. The Department has identified enterprise-wide cybersecurity situational awareness geared towards obtaining actionable intelligence as a critical need. Consequently, the Department has prioritized resources for a Department hub for this effort: the integrated Joint Cybersecurity Coordination Center (iJC3), provides a unified and standardized approach to cybersecurity data collection and shared analytics via real-time collaboration, while allowing individual Departmental Elements to develop unique cybersecurity strategies consistent with their respective mission objectives. The iJC3's ability to consolidate disparate cybersecurity functions and streamline information sharing enterprise-wide will strengthen the Department's overall security posture.

Presidential Policy Directive (PPD) 40, issued July 2016, identified Continuity of Operations (COOP) plan requirements and the need to include IT systems processes, and resources in COOP plan development. The Department will collaborate with DHS National Protection and Programs Directorate (NNPD) to protect and enhance the resilience of the Department's physical and cyber infrastructure. Additionally, under the Presidential Policy Directive-21, *Critical Infrastructure and Resilience*, the Department is the sector-specific agency for the Energy sector. Through CRISP, CESER, using technologies originally developed to defend DOE's networks, helps energy system owners and operators identify malicious traffic within their IT systems by analyzing the data streams and enhancing the analysis with classified DOE information sharing and cybersecurity tools. CRISP further provides them with a platform to voluntarily share cybersecurity threat data in near-real-time and receive machine-to-machine threat alerts and mitigation measures. The Electricity Information Sharing and Analysis Center (E-ISAC) manages CRISP with the goal to create a sustainable program owned and operated by the private sector. CESER seeks to expand Energy sector participation in data sharing efforts, and to advance analytic capabilities through CESERs Cyber Analytics Tools and Techniques (CATT) project. CESER also seeks to develop new OT capabilities by piloting real-time OT data sharing and analysis with a group of utilities in the Cybersecurity for the OT Environment (CYOTE) project.

MAJOR TASKS:

- Reach full operational capability for iJC3.
- Fully implement CDM enterprise-wide.
- Increase and enhance enterprise-wide sharing of analytics and real-time threat information to improve enterprise-wide cybersecurity situational awareness, incident detection, and tactical response.

- Improve visibility across operational energy infrastructure and develop a shared situational awareness capability among industry and with government.

Objective 2.4 RESPOND - *Rapid analysis of, and response to, anomalies and suspected events.*

To effectively combat advanced persistent threats, the Department needs to mature its cybersecurity Incident Management Program, to include expanding analytical forensics and response tactics, utilizing automated tools to streamline information technology security, improving incident management capabilities, and delivering training to frontline operators. Timely and accurate situational awareness is necessary to set operational priorities and match Department resources to requirements. To that end, in collaboration with Federal Government and Energy sector owners and operators, DOE is developing cutting-edge cybersecurity solutions to strengthen and coordinate incident response capabilities and share resources.

A key component of the Department's response effort is the iJC3, which also provides a unified and standardized approach to incident response and reporting across the Department. The iJC3 will be interoperable with CRISP's data flow. Interoperable cybersecurity solutions require common standards development.

Under the *DOE Multiyear Plan for Energy Sector Cybersecurity*, CESER and the OCIO will continue working with the Department's National Laboratories to develop reporting conventions and critical information requirements that facilitate a common operating picture, which internal and external stakeholders rely on during emergencies and steady-state operations. Meaningful public-private partnership is foundational to DOE's strategy. The Department has a unique responsibility with its National Laboratories to fund innovative research, development, and demonstration (RD&D) that cannot be economically justified by Industry and the private sector. The Secretary notes that America depends on the National Laboratories to "out-innovate" our adversaries. The Department considers RD&D investment as a game-changer for advancing the Nation's cybersecurity and, therefore, resilience today, and, as importantly, laying the foundation for a robust defense of the energy systems of tomorrow.

MAJOR TASKS:

- Adopt standard operating procedures for DOE cybersecurity incident reporting and response.
- Stand up the iJC3's classified capabilities.
- Conduct periodic testing of DOE cybersecurity incident response, to include enterprise-wide testing.
- Integrate energy sector cybersecurity data into iJC3.
- Develop, in collaboration with Energy sector owners and operators, information reporting requirements to form common operating picture.

Objective 2.5 RECOVER - *Develop and implement an incident triage, response, and recovery process to contain and eliminate cybersecurity threats.*

The Department needs to focus on identifying and remediating gaps between the requirements of its Continuity of Operations Program (COOP) and Disaster Recovery elements, and required IT and information resources support. The Department will strive to support cybersecurity elements and align its resilience efforts with PPD 40, Federal Continuity Directives (FCD) 1 & 2, and Federal Emergency Management Agency (FEMA) National Continuity Programs. COOP and Disaster Recovery Plan (DRP) rely on the availability of robust, reliable, and redundant IT infrastructure and IT resources, to include access to essential records. Given its dispersed geographic form and diverse functions, the Department does not have a unified Disaster Recovery plan. To ensure DOE Mission success, the OCIO will conduct a gap analysis of IT and IT resources necessary to enable the Department to perform its Primary Mission Essential Functions (PMEFs) and MEFs under all circumstances, to include cybersecurity attacks.

The OCIO will facilitate cybersecurity exercises that stress not only incident response processes and protocols, but recovery actions, to include reconstitution. Budgeting for contingencies must factor in the potentially prolonged unavailability or possible loss of vital IT infrastructure and systems, whether from a cybersecurity attack or natural disaster. DRP Test, Training, and Exercise (TTX) programs must be adopted and audited across the Department's multiple components elements.

MAJOR TASKS:

- Conduct gap analysis of required IT and IT resources necessary for COOP and the DRP.
- Ensure all mission-critical applications and infrastructure have sufficient continuity of operations and disaster recovery capabilities.
- Conduct realistic testing of critical IT failover systems.

GOAL 3 - TRANSITION FROM IT OWNER TO IT BROKER FOR BETTER CUSTOMER FOCUS

Objective 3.1 - CUSTOMER-FOCUSED CYBERSECURITY

Effective cybersecurity measures will be aligned with and tailored to, wherever possible, customers' specialized needs and ways of doing business. The more natural the fit and ease of adoption, the more effective the cybersecurity measures will be. The value proposition for cybersecurity measures must be clear to customers. Furthermore, continuous process improvements from both sides, cybersecurity defenders and customers, is required for long-term success. Informed and engaged customers are more likely to be invested partners in cybersecurity defense. Ideally, the collaborative partnership will lead to cybersecurity "baked in" from the ground-up. The process itself must be iterative and open, with issues identified and brought to the Department's IT, Information Resources Management, and Cybersecurity governance process for resolution without fear of punitive action.

MAJOR TASKS:

- Develop and implement iterative process for soliciting customer input/feedback and determining and understanding customer requirements and challenges.
- Provide value proposition for cybersecurity measures.
- Inject customer requirements into information flow for the Department's IT, Information Resources Management, and Cybersecurity governance process.
- Develop and implement cybersecurity measures that facilitate mission success through collaborative customer partnership where the customer is informed, engaged, and not afraid of punitive action for self-reporting.

GOAL 4 - EXCEL AS STEWARDS OF TAXPAYER DOLLARS

4.1 RISK-BASED APPROACH

Consistent with *FISMA* and E.O. 13800, and the *Cybersecurity Framework* the *Cybersecurity Strategy* follows a risk management methodology. The DOE CIO is the Senior Agency Official charged by the Secretary with Enterprise-wide responsibility for cybersecurity risk management. Pragmatism requires that the Department prioritize its limited resources to critical mission requirements while cognizant of the consequences of a cybersecurity event.

Cybersecurity risk will be considered in all phases of the Department's IT project planning, execution, management, and procurement. The Department needs to train, equip, and field invested network, system, and data owners who understand the value proposition of employing cybersecurity measures to increase the probability of their respective mission performance under all conditions. These owners are the actual acceptors and, consequently, holders of risk. Simultaneously, they are customers, and as such, they will engage with and be engaged by, in a collaborative manner, their cybersecurity service providers. In addition, and in alignment with the One Team, One Fight holistic approach, other components of the Department's ecosystem have significant complementary value to add in reducing cybersecurity risk, among them, for example, intelligence and counterintelligence (to include insider threat and supply chain risk management), enterprise assessments, privacy, and physical, personnel, and information (documents) security. The Department will be well-served by an integrated systems cybersecurity posture that establishes cybersecurity hygiene, yet has the flexibility to accommodate and ensure mission success across DOE's specialized task areas.

MAJOR TASKS:

- Provide cybersecurity risk management training to DOE IT stakeholders and cybersecurity professionals.
- Incorporate cybersecurity risk management into the Department's IT project management, IT procurement, and IT, IT Resources Management, and Cybersecurity governance processes.
- Ensure that the Department's IT, IT Resources Management, and Cybersecurity governance processes include Departmental elements with responsibility for, among others, intelligence and counterintelligence, enterprise assessments, privacy, and physical, personnel, and information (documents) security.
- Improve Departmental decision-making by improving and formalizing governance processes based on a risk management-based approach.
- Implement a comprehensive cybersecurity risk-based program plan to provide direction to DOE cyber defenders and IT professionals.
- Implement measures and metrics to track and analyze risk and the effectiveness of risk reduction measures across the enterprise.

Building a Sustainable Future

To sustain the *Cybersecurity Strategy* and the Department's Cybersecurity Program, the Department needs to address two critical resources: human capital and dedicated cybersecurity funding. With respect to the latter, DOE has allocated funding for ongoing cybersecurity programs to policy management, security awareness training, data collection, and reporting. The funding aligns with the *Cybersecurity Framework*, grouped into three budget lines:

1) Protecting Networks and Information—Protect;
2) Detect, Analyze, and Mitigate Intrusions—Detect and Respond; and
3) Shaping the Cybersecurity Environment—Identify and Recover.

Future funding is essential to provide additional capabilities and protections through the establishment or increased scope of program implementation, such as collaboration with DHS to improve security protection for information and CDM and expansion of the Department's HVA Program, and deployment of new and innovative cybersecurity products and services for protecting DOE IT infrastructure and information resources. As a start, per Congressional direction, responsibility for the Department's cybersecurity budget, knows as the Cyber Crosscut, has moved from the Office of the Chief Financial Officer to the OCIO. Modernized and automated systems will allow DOE to focus our workforce on the highest value add activities.

Concerning human capital, the Department needs dedicated cybersecurity professionals trained and equipped to defend the Department's IT assets and information resources. The complexity of that task is growing more difficult because of the sophistication of IT networks and systems, non-stop cyber probes and assaults, and the competitive pool of qualified cybersecurity professionals who receive more handsome compensation and benefits in the private sector. Given the double-digit projected growth of IT and cybersecurity jobs over the next decade, high-turnover, and ultra-competitive compensation and benefit packages, the Department needs to institute a plan for cybersecurity workforce development. The Department will not gloss over racial and gender underrepresentation: it must be intentional about expanding its recruiting programs to foster a more diverse applicant pool representative of the Nation. Further, in order to improve the technical ability of its cybersecurity professionals, the Department must emphasize continuous learning with measured outcomes and earmark training dollars as institutional investments with a high rate of return in terms of future performance.

Consistent with the National Initiative for Cybersecurity Education (NICE), the Department seeks to accelerate learning and skills development to address the shortage of skilled cybersecurity workers in both the public and private sectors. Consequently, the Department, among other things, has started a STEM Rising initiative and sponsors an annual Cyber Defense Competition, which, in April of 2018, saw nearly 200 students working in almost twenty-five blue teams competing in an exercise to protect natural gas networks against cyber-attacks from red team Industry and National Laboratory subject matter experts.

Following the President's direction pertaining to direct hire authority, the Department will utilize its Office of Personnel Management-approved authorities for direct hiring, competitive compensation and benefits (*e.g.*, hiring, performance, and retention bonuses, pay banding, telecommuting, and leave accommodation) to secure and retain talented professional to accomplish it mission.

Appendix A - Cybersecurity Strategic Implementation Plan (CSIP)

FY 2018 – FY2020

Introduction

The Department's aging Federal IT infrastructure, use of legacy systems and software, and urgent need for cybersecurity professionals are presenting significant cybersecurity and operational risks to its mission success. The *Cybersecurity Strategy* represents a paradigm shift from repairing and sustaining to investing, upgrading, and modernizing DOE's Federal IT infrastructure and associated systems and services, and executing a workforce development plan. The *Cybersecurity Strategy Implementation Plan* (*Plan*), completes the *Cybersecurity Strategy* by providing the operational blueprint for maturing the Department's cybersecurity activities consistent with principles, goals, and tasks, all grounded on widely-accepted risk management concepts. The *Plan* will be reviewed and updated annually in alignment with the Department's budget formulation and execution.

Overview

The Department's Chief Information Officer (CIO), leads the Department's Cybersecurity Program on behalf of the Secretary. Items relating to the Nation's Energy sector fall within the Office of Cybersecurity, Energy Security and Emergency Response Center (CESER).

Investing in improving the Department's Federal IT infrastructure will have a corresponding effect on the efficacy of its Cybersecurity Program. To that end, the Deputy Secretary has approved a Network Security Modernization Program for Federal IT that will—on an enterprise-wide basis:

(1) Improve the Department's cybersecurity posture.
(2) Provide scaled capacity commensurate with demand; establish IT enterprise capabilities allowing for commercial/managed service implementations of services with engineered and inherent cybersecurity capabilities, while providing foundational requirements for enhanced cybersecurity tools, products, and capabilities; and lead to cost-efficiencies.

Further, partnering with Industry through CESER, utilizing the superlative talent across the Department, to include its National Laboratories, and collaborating with Federal departments and agencies will strengthen DOE's cybersecurity measures and provide cost-savings from adopting common training platforms, deploying Executive Branch-wide tools, such as Continuous Diagnostics and Mitigation (CDM), and adopting in internally developed, innovative solutions to unique DOE requirements.

Key activities for FY 2018 to FY 2020 include:

- Executing Network Security Modernization Program projects.
- Collaborating with DHS to implement the CDM Program enterprise-wide by 2020.
- Integrating the HVA Program with iJC3 functions.
- Deploying cutting edge cybersecurity products and services across the enterprise.
- Sharing cybersecurity information enterprise-wide on a timely basis under a common taxonomy.

Cybersecurity Funding

Programs and activities associated with the OCIO cybersecurity fall under three budget lines below that align with the *Cybersecurity Framework*.

- PROTECT—Protecting Networks and Information
- DETECT and RESPOND—Detect, Analyze, and Mitigate Intrusions
- IDENTIFY and RECOVER—Shaping the Cybersecurity Environment Strategic Implementation

Additionally, the Department has mapped this plan to the *Cybersecurity Framework* Functions and component categories in Appendix C.

IT Program Management Office

In order to successfully execute this *Plan*, program management discipline and a Cybersecurity Program Office, dedicated funding, representative and transparent governance, a high caliber workforce, and continuous evaluation and refinement are essential keys. The OCIO has established an enterprise-wide IT Program Management Office (ePMO) to provide support to program including the Cybersecurity Program Office. The ePMO will operate under the auspices of DOE Order 415.1, *Information Technology Program Management* and its related documents.

Cybersecurity Program Office

To execute the *Cybersecurity Strategy* and this *Plan*, the CIO realigned the OCIO Cybersecurity Program Office, designated as IM-30, to better align with *FISMA* and NIST's *Cybersecurity Framework* and to leverage industry best-practices. IM-30 is charged with assisting the CIO with conducting oversight of cybersecurity programmatic activities enterprise-wide. The IM-30 organizational structure, with functional breakdown, is provided as Appendix E to this *Plan*.

FITARA-driven Collaboration

IT procurements, enterprise-wide, along with IT budgets, are subject to the CIO's approval under the *Federal Information Technology Acquisition Act* (FITARA), implementing direction for which is found in Department orders and in Chapter 39.3 of the Department's *Acquisition Guide FY2018*. The Department's Senior Procurement Executive works closely with the CIO to ensure that DOE procurement processes minimize administrative burdens and to centrally track and approve all IT purchases to reduce redundancies and reduce supply chain risks associated with IT procurements.

Likewise, review of the Department's IT and cybersecurity budget requests and funding execution is a joint-venture between the OCIO and the Department's Office of the Chief Financial Officer (OCFO). The IT Investment Portfolio, which collects investment data within the OCIO-managed electronic Capital Planning and Investment Control (eCPIC) tool, serves as the Department's IT Budget data of record. Subject matter experts from each office convene to analyze cybersecurity funding, known as the Cybersecurity Crosscut, which is included in the Department's annual President's Budget submission.

The OCIO will document clear, consistent, and visible processes that allow the efficient use of funding, to fulfil the responsibility of being accountable to the enterprise in addition to being good stewards of tax payer dollars. Notably, the Department received OMB approval to submit a request for funding under the new Technology Modernization Fund [more detail] for consolidation of the Department's numerous email systems.

Cybersecurity Governance

The CIO is also examining ways to improve the Department's IT and cybersecurity governance structure and processes, starting with the Deputy Secretary-chaired Cyber Council. In addition, the OCIO is leading efforts to update the Department's IT and cybersecurity orders, beginning with DOE Order 205.1, *Cyber Security Program*.

Workforce Recruitment

The CIO is acutely aware that recruiting and retaining a world-class workforce is the lynchpin for executing this *Plan*. Accordingly, in addition to the CIO's FITARA's authority to approve the hiring of CIO or CIO-like positions in the Department and participate in the performance reviews of the same [NOTE currently approx. 13 slots], the Deputy Secretary has directed that the CIO review all new hires of General Schedule 2210 positions. In concert with the Office of the Chief Human Capital Officer, the CIO is responsible for the Department's use of direct hire authority, and expanding the Department's use of compensation and benefits and training funds, to recruit, develop, and retain top IT and cybersecurity talent.

Summary

The Cybersecurity Strategic Implementation Plan, outlined in latter sections, has a three-year planning horizon and will be revisited annually, or, more frequently as required by the Cyber Council to keep up with the ever-changing cybersecurity landscape and respond rapidly to evolving national security imperatives.

The Performance Plan in Appendix G represents the substance of this Plan. It provides the operating details on the Department's IT and cybersecurity goals, objectives, budget lines, and associated activities. In particular, it incorporates major tasks and activities over a 2-year timeline, with the first year representing the current budget year, FY 2018. The second year includes funded and unfunded prioritized requirements for FY 2019.

Goals, Objectives, Major Tasks and Activities

Goal #1 - Deliver High-Quality IT and Cybersecurity Solutions

OBJECTIVE 1.1 - SECURE and RELIABLE INFORMATION ACCESS

Major Tasks:
a. Ensure the availability of and access to systems, networks, and information resources that enable DOE to perform the full lifecycle of its mission-essential functions. ***Activities:*** **Secure Communications for International Travel (Safe Passage) –** 1) The Safe Passage Program addresses multiple security and risk-related issues with respect to senior DOE officials traveling to foreign countries while on official business. 2) These vulnerabilities, if exploited, could provide reach-back to the internal DOE network upon a traveler's return and potentially be leveraged by remote adversaries to ex-filtrate data, monitor critical communications between senior staff, or in other malicious ways that would significantly impact or degrade the security and effectiveness of the DOE mission. 3) The program reduces travel devices as potential attack vectors on the DOE IP networks, foster risk awareness and best practices for foreign travel, and protect DOE information resources and assets using a dedicated pool of mobile devices for foreign travel, and additional staffing and tools to perform pre-trip and post-trip provisioning and forensic analysis of the devices.
b. Provide service providers, customers, and stakeholders with timely and accurate information necessary for them to make informed risk management-based decisions.
c. Ensure that Departmental High Value Assets (HVAs) are protected by cybersecurity and physical controls, as well as, adequately managed and resourced throughout their lifecycle.
d. Strengthen the cybersecurity of corporate data and information resources data centers.
e. Leverage new network paths and secure data transfer technologies to increase internal and external information flow across DOE sites and operating environments.
f. Integrate Supply Chain Risk Management (SCRM) with mission-oriented, risk-based protections that support information technology-based services, external access, and collaboration.
g. Provide enhanced role-based cybersecurity training requirements and programs to ensure that users are fully cognizant of their responsibilities for protection of the Department's information resources.

Goal #2 - Continually Improve Cybersecurity Posture

OBJECTIVE 2.1 IDENTIFY – Enhance organizational capabilities to manage the cybersecurity risk.

Major Tasks:

a. Develop policies that direct the establishment of cybersecurity hygiene through the use of automated tools, strengthening of internal controls, and standardization of processes and reporting to reduce the cost and management complexity of cybersecurity functions.

Activities:

1) *Reporting – Data Collection, Analysis, and Metrics –*

a) Analyze data to identify successful strategies, systemic weaknesses, anomalies, and root causes to ensure effective enterprise risk management and cybersecurity programs.

b) Address weaknesses in FISMA reporting processes to ensure that DOE's security posture is accurately reported, identify weak links in the overall posture, and open lines of communication to facilitate information sharing.

c) Evaluate the DOE organization and its components, define effective metrics, and identify where additional effort is needed to further mature existing programs.

2) ***Cyber for EITS (Assessment and Authorization (A&A)) –***

a) Provide A&A in cybersecurity control implementation, management and monitoring of the Energy Information Technology Services (EITS) Enclaves and Subsystems to ensure compliance with FISMA and NIST requirements.

b) OCIO is planning to transition to Ongoing Authorization (OA) as a key part of the EITS Authorization Process that leverages the Information Security Continuous Monitoring (ISCM) strategy and program.

c) The OA plan will utilize the guidance and best practices available from OMB, NIST, DHS and others. Maturation of the EITS ISCM is anticipated to provide efficiencies in future years.

3) ***Identify and Recover High Value Assets (HVA) –***

a) Implement enhanced controls and expand assessments to support Plan of Actions and Milestones (POAM) remediation.

b) Activities include direct review of security requirements supporting HVA related IT Modernization efforts to support security enhancements in DHS specified risk areas: System Boundaries, Network Segmentation, Governance and Risk, Identity and Access management and Continuous Monitoring.

b. Adopt standards and processes that facilitate and accelerate the secure integration of innovative IT solutions.

c. Conduct assessments to ensure that integration of new IT hardware, software, and firmware meet cybersecurity standards (along with legal and regulatory requirements) to prior to integration into the Department's information ecosystem.

d. Overseeing and analyzing assessments to make an overall assessment of the Department's risk posture.

OBJECTIVE 2.2 PROTECT - Develop and implement enterprise controls to reduce risk and increase resilience; promote enterprise cybersecurity awareness through workforce development and training.

Major Tasks:

a. Design and implement cybersecurity requirements, measures, and solutions that harden DOE's infrastructure and network environment, thereby increasing protection of its information resources.

Activities:

1) ***Requirements Analysis and Integration –*** Collect and build the enterprise architecture view and the list of Technical and Cybersecurity Requirements that inform implementation. In later stages of the project lifecycle, maintain status on cybersecurity certifications and controls implemented, hosting agreements, contract consolidations, and implementation approaches. Continue design of the Shared Services architecture and process workflows for requested IT services across the enterprise. Enterprise implementation of like products with separate installations will demonstrate cost savings and value of moving to shared government solutions.

2) ***iJC3 Cyber Operational Technology –*** Support the discovery, cataloging, assessment, and monitoring of Operational Technology.

3) Network Security Modernization – Modernize DOE's Network Security through a secure, robust, and capable network, built on interoperable standards and architecture principles. Projects support the DOE enterprise by improving Cybersecurity, scale capacity commensurate with demand, and establish the foundation for future IT enterprise capabilities, include:

   a) ***Core Infrastructure Service Expansion –*** Support the expansion of core Energy IT Services (EITS) infrastructure services, increase network bandwidth, and project activities in support of transitioning additional customers onto DOE enterprise cloud and managed services. Addresses upgrades to the email gateway infrastructure, DOE Wide Area Network (WAN) upgrades to support new customer sites, and project activities to support the migration of customers from the DOE Federal enterprise.

   b) ***Application Rationalization –*** Application Rationalization seeks to identify applications within the enterprise, verify their mission need, consolidate, and/or eliminate duplicative applications, and identify more efficient means for application delivery such as app-virtualization. DOE can streamline its portfolio of applications with the goal of improving efficiency, reducing complexity and redundancy, and lowering the cost of ownership. The DOE continues to improve their inventories and processes to rationalize their applications.

   c) ***Desktop as a Service –*** Transition from on-premises desktop services to a managed cloud Desktop-as-a- Service (DaaS) solution.

   d) ***Digital Business Technology Platform –*** The digital business platform provides a single unit purchased from a vendor that incorporates information systems platform, customer experience platform, data and analytics platform, data management programs, Internet of Things (IoT) platform, and ecosystems platform. The goal is to create an interoperable set of services that can be brought together to create applications, apps and workflows in support of DOE missions. This creates a symbiotic collection of technology capabilities and components that form a platform. A services-first versus applications-first mindset is one of the main attributes of a loosely coupled, interoperable platform.

Major Tasks:

b. Execute a Department-wide approach to ICAM to control accessibility of Department information resources, systems, and facilities.

Activities: **Identity, Credential, and Access Management (ICAM) –**

1) Fulfil the requirement for Personal Identity Verification (PIV) and other Identity Assurance Level (IAL)/Federation Assurance Level (FAL)/Authenticator Assurance Level (AAL) for network access for privileged and un-privileged accounts. Enable expansion of DOE's digital identity repository to serve as the primary identity source for implementation of CDM phase 2.

2) Expand federated authentication services for DOE sites enabling use of the proper credential, based on a role-based risk assessment and federation of the authentication service to external federated authentication services including bi-directional federation with OMB MAX.

3) Align and adopt credentials based on NIST SP 800-63-3 standard using commercial solutions to meet AAL2 and AAL3.

4) Implement derived credentials used on mobile and non-GFE (Government Furnished Equipment) at the appropriate assurance level for USAccess implemented derived PIV credential service for shared services customers.

c. Augment and support enhanced cybersecurity services at all Department sites.

Activities: **Cyber Supply Chain Management –**

1) Sustains an enterprise Supply Chain Risk Management program (SCRM) that provides proactive, defense-in-depth supply chain security support for the DOE Enterprise through risk modeling and threat assessment.

2) The Program also provides capabilities that guide, educate, and manage supply chain risks to National Security Systems (NSS) and Information and Communications Technology (ICT) components and includes shared services, a common lexicon, and best practice procedures in procurement, delivery, and deployment of IT products and services that are used across the enterprise.

d. Provide relevant training, education, and awareness to all DOE employees regarding cybersecurity threats, risks, and impacts, thereby encouraging greater individual accountability and responsiveness.

e. Develop a highly capable cybersecurity workforce through specialized, role-based training and development.

Activities: **Coordinated Cyber Response –** Cyber Fire develops cyber incident responder specialized skills needed to defend against and mitigate cyber threats through extensive training and provides advanced teams of incident responders to respond to escalated cyber incidents.

f. Improve current cybersecurity training curriculum, to include human performance assessment programs.

OBJECTIVE 2.3 DETECT - Develop tools and processes to accelerate notification of cybersecurity threats.

Major Tasks:
a. Reach full operational capability for iJC3. ***Activities:*** **Integrated Joint Cybersecurity Coordination Center (iJC3) –** 1) The iJC3 provides cybersecurity threat analysis in coordination with DOE National Laboratories; conducts attack trending and tracking of advanced persistent threats; and distributes threat information and indicators of compromise to DOE entities in an automated manner. 2) Integrates DOE Incident Management capabilities and coordinates all enterprise activities including prevention, detection, containment, and recovery on both unclassified and classified networks through internal partnerships with the National Nuclear Security Administration (NNSA) and Counterintelligence and Intelligence (IN). 1) The iJC3 also coordinates communications for cybersecurity events and cyber emergency response with United States Computer Emergency Readiness Team (US-CERT) and other agency partners.
b. Fully implement CDM enterprise-wide.
c. Increase and enhance enterprise-wide sharing of analytics and real-time threat information to improve enterprise-wide cybersecurity situational awareness, incident detection, and tactical response. ***Activities:*** 1) ***Cyber Intelligence –*** The Cyber Federated Model (CFM) is an iJC3 service that provides machine-to-machine sharing of cyber threat intelligence, speeding up proactive defense, and distributed detection for the National Laboratories and site offices. CFM can deliver signatures and indicators of compromise to automatically update cyber defenses, such as intrusion detection systems, intrusion prevention systems, and firewalls. 2) ***Detection and Response for HVAs –*** Support detection through increased assessments, tracking findings and remediation, and coordination of external auditing and reporting for DHS and OMB. Resources to provide analysis, prioritization, visibility, and response for HVAs. 3) ***Cyber for EITS –*** Continuous monitoring, cybersecurity assurance and accreditation, and information systems security officer support for EITS customers.
d. Improve visibility across operational energy infrastructure and develop a shared situational awareness capability among industry and with government.

OBJECTIVE 2.4 RESPOND - Rapid analysis of, and response to, anomalies and suspected events.

Major Tasks:
a. Adopt standard operating procedures for DOE cybersecurity incident reporting and response.
b. Stand up the iJC3's classified capabilities.
c. Conduct periodic testing of DOE cybersecurity incident response, to include enterprise-wide testing.
d. Integrate energy sector cybersecurity data into iJC3.
e. Develop, in collaboration with Energy sector owners and operators, information reporting requirements to form common operating picture.

OBJECTIVE 2.5 RECOVER - Develop and implement an incident triage, response, and recovery process to contain and eliminate cybersecurity threats.

Major Tasks:

a. Conduct gap analysis of required IT and IT resources necessary for COOP and the DRP

b. Ensure all mission-critical applications and infrastructure have sufficient continuity of operations and disaster recovery capabilities.

Activities:

1) ***Operationalize new products –*** Operationalize new Cybersecurity products or services, such as hardware, software, applications, and equipment, designed to protect the DOE IT infrastructure.

2) ***Network Security Modernization –*** Modernize DOE's Network Security through a secure, robust, and capable network, built on interoperable standards and architecture principles. Projects that make up the initiative include:

   a) ***Continuity of Operations/Disaster Recovery Planning –*** enable the integration of the unclassified Security Operations Center (SOC) and Incident Response capabilities in DOE's Continuity of Operations and Disaster Recovery planning to ensure Unified Coordination Structure (UCS) response to any cybersecurity event. Full integration of these capabilities under the Unified Coordination Structure enables the department to manage a cybersecurity event utilizing and incorporated with the UCS response to a stand-alone incident, or as part of a larger Continuity or Disaster Recovery event. Also provides for the initial year licensing to expand the use of the DOE Alert, Warning, Accountability, and Response (DOE-AWARe) system across the DOE enterprise, and for implementation of an expanded accountability module within the system. DOE-AWARe utilizes a cloud-based service and supports notification and accountability for emergency and continuity events.

   b) ***Cybersecurity Infrastructure Upgrades –*** Planned upgrades for the deployment of additional infrastructure in support of the CDM program to provide redundancy and high-availability for CDM capabilities previously deployed within the enterprise. The funding provided to DOE by DHS does not provide for redundancy and high-availability for CDM capabilities deployed in CDM phase 1 and 2. Supports technology refresh, and expansion of the EITS Security Operations Center infrastructure supporting PCAP (packet capture), SIEM (Security Information and Event Management), and the network security and Incident Response capabilities.

c. Conduct realistic testing of critical IT failover systems.

Goal #3 - Transition from IT Owner to IT Broker for Better Customer Focus

OBJECTIVE 3.1 CUSTOMER-FOCUSED CYBERSECURITY

Major Tasks:
a. Develop and implement iterative process for soliciting customer input/feedback and determining and understanding customer requirements and challenges.
b. Provide value proposition for cybersecurity measures.
c. Inject customer requirements into information flow for the Department's IT, Information Resources Management, and Cybersecurity governance process.
d. Develop and implement cybersecurity measures that facilitate mission success through collaborative customer partnership where the customer is informed, engaged, and not afraid of punitive action for self-reporting.

Goal #4 - Excel as Stewards of Taxpayer Dollars

OBJECTIVE 4.1 RISK-BASED APPROACH

Major Tasks:
a. Provide cybersecurity risk management training to DOE IT stakeholders and cybersecurity professionals.
b. Incorporate cybersecurity risk management into the Department's IT project management, IT procurement, and IT, IT Resources Management, and Cybersecurity governance processes.
c. Ensure that the Department's IT, IT Resources Management, and Cybersecurity governance processes include Departmental elements with responsibility for, among others, intelligence and counterintelligence, enterprise assessments, privacy, and physical, personnel, and information (documents) security.
d. Improve Departmental decision-making by improving and formalizing governance processes based on a risk management-based approach. ***Activities:*** **Planning, Policy, and Risk Management –** • Organize and capture enterprise cyber risk management goals to make informative, risk-based cybersecurity decisions. • By providing policy, guidance, strategies, and implementation plans through an exclusive Department Enterprise Risk Management- Cybersecurity (ERM-CS) initiative. OCIO works closely with Department Programs and Sites to develop, document, and deploy fundamental approach(s) to cybersecurity and enterprise risk management. • OCIO leverages OMB Circular A-123 risk profiles containing cybersecurity risks. Strategic planning is also leveraged to identify critical cybersecurity gaps, establish priorities, and determine appropriate actions to improve the Department's cybersecurity posture.
e. Implement a comprehensive cybersecurity risk-based program plan to provide direction to DOE cyber defenders and IT professionals. ***Activities:*** **Protect High Value Assets –** Develop and implement an HVA Risk Management Dashboard enabling integration of automated information feeds from enterprise risk platforms, assessment findings, and threat intelligence providing increased visibility of enterprise risk to the Department's most critical assets.
f. Implement measures and metrics to track and analyze risk and the effectiveness of risk reduction measures across the enterprise.

Strategic Implementation

DOE's Cybersecurity Strategy Implementation Plan (CSIP) establish a formal Enterprise-wide Cybersecurity Program and Program Office. The organization of DOE's Cybersecurity Program Office can be found in Appendix E. The OCIO Cybersecurity Program Office, designated as IM-30, was recently re-aligned to better perform functions required by the OCIO Modernization Strategy, to better align with FISMA requirements, and to better align with the NIST Cybersecurity Framework. In addition, there is an extended Cybersecurity Program Office across DOE given DOE's unique organization and mission. The extended Cybersecurity Program Office includes representation from CESER, NNSA, major headquarters elements and National Laboratories, plants, sites, program offices, and the Power Marketing Administrations (See Appendix F).

DOE's CSIP incorporates major tasks and activities over a 1 to 2 year timeline. The first year represents the current budget year, FY2018. The second year includes funded and unfunded prioritized requirements for FY 2019. A high-level 2 year timeline is included at Appendix G.

Program Management

The OCIO Enterprise Project Management Office (ePMO) leverage well-established principles to gain efficiencies and improve customer and stakeholder engagement across the enterprise. Effective IT governance empowers program offices to make decisions about their IT requirements, while providing guidance and support to ensure their success.

An important CSIP component is that DOE OCIO must implement, coordinate, facilitate, and manage a successful cybersecurity development and procurement program. This effort will incorporate strategic sourcing initiatives, procurement support, procurement oversight, program support, and ensure compliance with good business practices and applicable regulations and policies through oversight reviews.

DOE OCIO's implementation of these strategic plan initiatives, coupled with the sound execution of procurement operations, will enable success and directly support the overall DOE mission and goals. A sound procurement strategy within the DOE OCIO includes:

- Research and planning to add value to sourcing, implementation, and results;
- Collaborative efforts across the enterprise to strengthen solutions, productivity, and efficiency;
- Governance and project management to ensure delivery is on schedule, on budget, and to specification; and
- Accountability and transparency to identify and manage challenges.

Cybersecurity Funding

The Federal IT Acquisition Reform Act (FITARA) sets forth the DOE OCIO's responsibilities to approve, oversee, and report IT spending across the enterprise. The CIO responsibilities were reinforced in the Executive Order Enhancing the Effectiveness of Agency CIOs (15-May-2018). The Information Management Governance Board (IMGB) process is an integral piece of the DOE governance model and enterprise architecture and contributes to the effectiveness of that model.

The DOE OCIO creates and maintains a healthy operational budget to efficiently spend and successfully achieve its mission. The DOE receives appropriated funds that are congressionally mandated to support DOE OCIO's annual requirements for cybersecurity for the enterprise. This funding enables the procurement of software, hardware, labor, services, applications, systems, projects, and the required

security to fulfill the DOE OCIO Mission.

The DOE OCIO sustains the necessary processes and guidance to allow the proper control of all funds disbursed through Planning, Programming, Budgeting and Evaluation (PPBE) processes. The DOE OCIO will document clear, consistent, and visible processes that allow the efficient use of funding as part of its accountability to the enterprise and good stewardship of tax payer dollars. The DOE OCIO works with the IMGB to evaluate the feasibility and acceptability of projects that provide value to the organization within the CIO budget.

Continual Plan Review and Revision (Continual Improvement)

This strategic implementation plan has a three-year planning horizon and will be revisited annually – or more frequently if needed through the IMGB and Cyber Council forums. Regular reviews and updates reflect the continued need for DOE to keep up with the ever-changing cybersecurity landscape and respond rapidly to the evolving imperatives of national security.

Appendix B - Strategic Alignment

U.S. Department of Homeland Security (DHS) Cybersecurity Strategy

Like the Department of Homeland Security's Cybersecurity Strategy, DOE's cybersecurity posture leverages enterprise capabilities to manage cybersecurity risks strategically. DOE's risk management approach encompasses risk prioritization, cost-effectiveness, innovation and agility, collaboration, global approach, balanced equities, and national values. DOE empowers the cybersecurity programs to succeed by integrating privacy protections and, therefore, reduce organizational and systemic vulnerabilities to malicious cyber activity. This empowers stakeholders to make informed risk-management decisions and improves their cybersecurity.

IT Modernization

DOE is modernizing its IT to enhance mission effectiveness and reduce its cybersecurity mission risks. The cybersecurity objectives address the risk mitigation of data, systems, and networks by implementing industry-standard cybersecurity capabilities. This cybersecurity strategy provides measurable management of asset security by implementing capabilities that provide observational, analytical, and diagnostic data of DOE's cybersecurity. Protection of DOE's networks and sensitive government and citizen data are a priority. The implementation of credential and access management capabilities strongly align to DOE's focus to ensure users only have access to the resources necessary for their job function.

Federal IT Acquisition Reform Act (FITARA)

FITARA expanded the role, responsibilities, and authorities of the CIO to provide enterprise-wide direction for managing IT and cybersecurity. FITARA provides that the CIO is to report directly to the Secretary and Deputy Secretary for carrying out certain CIO functions. It also provides best practices in IT management and cybersecurity. Additionally, the "Protect" metrics of the PortfolioStat Performance Metrics strongly align to this cybersecurity strategy.

Office of Management and Budget (OMB) Circular A-130

This cybersecurity strategy aligns to OMB Circular A-130, which mandates that DOE manage Federal information as a strategic resource. The circular requires: 1) Real-time knowledge of the environment, continuous assessment of DOE systems, and built-in security and privacy in updates and re-designs; 2) Proactive risk management by modernizing the way DOE identifies, categorizes, and handles risk to ensure both privacy and security; and 3) Shared responsibility to ensure everyone remains responsible and accountable for assuring privacy and security of information – from managers to employees to citizens interacting with government services.

Federal Information Security Management Act (FISMA)

This cybersecurity strategy aligns to FISMA, effectively implementing an agency-wide information-security program that includes periodic risk assessments. It also bases policies and procedures on risk assessment and reducing information security risks to an acceptable level. This strategy addresses information security throughout the lifecycle of each system and compliance with applicable requirements. There is a focus on providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate, and furthering security awareness training to inform personnel of information security risks and of their responsibilities for complying with Departmental policies and procedures.

National Initiative for Cybersecurity Education (NICE)

This cybersecurity strategy aligns to the National Initiative for Cybersecurity Education (NICE). The strategy's objectives accelerate learning and skills development to address the shortage of skilled cybersecurity workers in both the public and private sectors. By strengthening education and training across the ecosystem, DOE emphasizes learning, measures outcomes, and diversifies the cybersecurity workforce, nurturing a diverse learning community. Finally, this strategy guides career development and workforce planning to support cybersecurity market demands and enhances recruitment, hiring, development, and retention of cybersecurity talent.

Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Protecting America's energy systems from cyber-attacks and other risks is a top national priority. This *Cybersecurity Strategy and Implementation Plan (CSIP or the Plan)* identifies collaborative actions to leverage within the Department to reduce cyber risks in the U.S. energy sector by pursuing high-priority activities that are coordinated with other DOE offices, and with the strategies, plans, and activities of the Federal Government and the energy sector. The *Plan* identifies the goals, objectives, and activities that DOE will pursue over the next five years to reduce the risk of energy disruptions due to cyber incidents.

Reliable energy and power is the cornerstone of our advanced digital economy and is essential for critical operations in transportation, water, communications, finance, food and agriculture, emergency services, and more. Today, any cyber incident has the potential to disrupt energy services, damage highly specialized equipment, and threaten human health and safety. As nation-states and criminals increasingly target energy networks, the Federal Government must help reduce cyber risks that could trigger a large-scale or prolonged energy disruption. While the *Plan* outlines activities specifically for DOE, we look forward to conducting these efforts in close partnership with the energy industry and Federal and non-Federal partners throughout the nation.

President's Management Agenda

The *President's Management Agenda* lays out a long-term vision for modernizing the Federal Government in key areas that will improve the ability of all agencies to deliver mission outcomes, provide excellent service, and effectively steward taxpayer dollars on behalf of the American people. The agenda outlines three key drivers of modernizing government for the 21st century:

1. **Modern information technology** that helps Government meet customer expectations and keep data and systems secure in the digital age.
2. **Data, accountability, and transparency initiatives** that deliver visibly better results to the public, while improving accountability to taxpayers.
3. **A Workforce for the 21st century** that enables senior leaders and front-line managers to nimbly align staff skills with evolving mission needs.

This CSIP aligns with the *President's Management Agenda* key drivers focusing on the cybersecurity aspects. The *President's Management Agenda* associated Cross Agency Priority (CAP) Goals includes the goal to Modernize IT to Increase Productivity and Security, under which the majority of cybersecurity efforts fall. The Department strives toward achievement of this goal to build and maintain more modern, secure, and resilient IT to enhance mission delivery and productivity – driving value by increasing efficiencies of Government IT spending while potentially reducing costs, increasing efficiencies, and enhancing citizen engagement and satisfaction with the services we provide. Appendix H provides the mappings of *President's Management Agenda* IT Modernization Key Milestone and related capability with the DOE Strategy and Implementation Plan Goals, Objectives, and Major Tasks.

Presidential Policy Directive 41 (PPD-41)

(PPD-41), United States Cyber Incident Coordination (July 2016), outlines three concurrent lines of effort to respond to any cyber incident involving government or private-sector entities: threat response; asset response; and intelligence support and related activities. CESER, in implementing the Department's role as the SSA for the energy sector, will coordinate Federal Government efforts to understand the potential business or operational impact of any cyber incident on critical infrastructure in the energy sector. If a significant incident directly impacts DOE operations, DOE OCIO will initiate a fourth line of effort to

directly address the cyber-attack. In addition, DOE will participate in national policy and operational coordination efforts for significant cyber incidents affecting the energy sector.

Executive Order 13800 (EO 13800)

EO 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017), directs DOE and other Sector-Specific Agencies to examine how Federal authorities and capabilities can be better used to support the cybersecurity risk management efforts of critical infrastructure entities, particularly those assets designated at greatest risk under Section 9 of EO 13636. The order also directs DOE to work with DHS, the Director of National Intelligence, and other partners to assess U.S. readiness to manage a prolonged power outage due to cyber-attack and any gaps in assets or capabilities needed to mitigate potential consequences.

Appendix C: NIST Cyber Security Framework Functions and Categories

This Cybersecurity Strategy and Implementation Plan aligns with the NIST CSF Functions. The table below provides the Fiscal Year (FY) allocations for FY18 (Appropriated) and FY19 (Requested) across the five functions based on DOE cybersecurity cross cut information. The NIST CSF Functions are used as key divisions for FISMA Metrics to track performance and OMB Capital Planning and Investment Control (CPIC) in planning, programming, budget and execution processes. To provide some further insight into cybersecurity the Department provides the below NIST CSF Category mapping for its Goals and Objectives.

Function	FY18 (Appr)	FY19 (Req.)		Category	DOE Cybersecurity Goal & Objective & Major Task From Implementation Plan
IDENTIFY (ID)	16%	22%	AM	Asset Management	Goal 2 - Objective 1 – Major Task a
			BE	Business Environment	Goal 2 - Objective 1 – Major Task b
			GV	Governance	Addressed through this document Goal 4 - Objective 1 – Major Task c
			RA	Risk Assessment	Goal 2 - Objective 1 – Major Task c
			RM	Risk Management Strategy	Goal 2 - Objective 1 – Major Task d Goal 4 - Objective 1 – Major Task a, b, d, e, f
			SC	Supply Chain Risk Management	Goal 1 - Objective 1 – Major Task f
PROTECT (PR)	35%	33%	AC	Identity Management and Access Control	Goal 2 - Objective 2 – Major Task b
			AT	Awareness and Training	Goal 2 - Objective 2 – Major Task d, e, f
			DS	Data Security	Cross cutting coverage in Major Tasks
			IP	Info. Protection Processes & Procedures	Cross cutting coverage in Major Tasks
			MA	Maintenance	Cross cutting coverage in Major Tasks
			PT	Protective Technology	Goal 2 - Objective 2 – Major Task a, c
DETECT (DE)	25%	25%	AE	Anomalies and Events	Goal 2 - Objective 3 – Major Task c, d
			CM	Security Continuous Monitoring	Goal 2 - Objective 3 – Major Task b
			DP	Detection Processes	Cross cutting coverage in Major Tasks
RESPOND (RS)	20%	15%	RP	Response Planning	Goal 2 - Objective 4 – Major Task a, c
			CO	Communications	Goal 2 - Objective 4 – Major Task b, d, e
			AN	Analysis	Cross cutting coverage in Major Tasks
			MI	Mitigation	Cross cutting coverage in Major Tasks
			IM	Improvements	Cross cutting coverage in Major Tasks
RECOVER (RC)	4%	5%	RP	Recovery Planning	Goal 2 - Objective 5 – Major Task a, b, c
			IM	Improvements	Cross cutting coverage in Major Tasks
			CO	Communications	Cross cutting coverage in Major Tasks

The Department Notes:

- Many investments may cut across more than one Function and/or Category and a primary Function and category was selected.
- A differing perspective of the NIST CSF Function in some OMB CPIC processes and reporting involve Capabilities within each NIST CSF Functions.
- Based on budget structure and areas of responsibility the FY19 percentages exclude consideration of requested funding for CESER and the NNSA Enterprise Security Computing.
- Percentages also exclude DHS provided seed funding for CDM implementation across the department.

Appendix D: Cyber Strategy Guiding Documents

The ***DOE Cybersecurity Strategy*** incorporates more than 25 guiding documents, including Federal mandates and directives to strengthen information sharing and safeguarding. The core list of documents is as follows:

1. 2015 Report on Configuration Management at the National Laboratories and Plants
2. 25 Point Implementation Plan to Reform Federal IT Management
3. Cybersecurity Risk Information Sharing Program
4. Department of Homeland Security Cybersecurity Strategy (Draft, March 7, 2018)
5. Department of Homeland Security Information Sharing and Safeguarding Strategy
6. Digital Government Strategy Report for the DOE
7. Digital Government: Building a 21st Century Platform to Better Serve the American People
8. DOE Information Resources Management (IRM) Strategic Plan FY2014-2018
9. DOE Information Technology Modernization Strategy
10. DOE Laboratories: Leadership in Green IT
11. DOE National Laboratories and Plants: Leadership in Cloud Computing
12. DOE Office of Electricity Delivery and Energy Reliability, Energy Sector Cybersecurity Framework Implementation Guidance
13. DOE Office of the CIO 120-Day IT Service Delivery Study
14. DOE Office of the CIO Enterprise Roadmap
15. DOE Office of the CIO FY2013 Human Capital Management Plan
16. DOE Office of the CIO Strategic Focus Points
17. DOE Office of the CIO Technology Modernization Strategy and Plan (March 12, 2018)
18. Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
19. Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
20. Executive Order Enhancing the Effectiveness of Agency CIOs (15-May-2018)
21. Federal Continuity Directives (FCD) 1 & 2
22. Federal Information Security Modernization Act of 2014 (FISMA)
23. Federal Information Technology Acquisition Reform Act (FITARA)
24. FY 2018 Budget Justification - Department of Energy
25. FY 2019 Budget Justification - Department of Energy
26. Government Accountability Office (GAO): Report to Congressional Requesters, Federal CIOs: Reporting to OMB Can Be Improved by Further Streamlining and Better Focusing on Priorities
27. Management and Oversight of Federal Information Technology (OMB Memorandum for Heads of Executive Departments and Agencies, 2015)
28. National Information Exchange Model
29. NIST Framework for Improving Critical Infrastructure Cybersecurity
30. NIST Risk Management Framework (RMF)
31. NNSA IM Strategic Implementation Plan 2016
32. Office of the Director of National Intelligence Strategic Intent for Information Sharing
33. OMB Circular A-130, Management of Federal Information Resources
34. OMB Memorandum M-16-04, OMB Cybersecurity Strategy and Implementation Plan for Federal Civilian Government

Appendix E: DOE Cybersecurity Program Office (IM-30) May 2018

The Office of the Chief Information Officer (OCIO) leads the Department's cybersecurity program on behalf of the Secretary and in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). This includes protecting DOE networks and information; detecting, analyzing, and mitigating intrusions; providing continuous monitoring of the network and infrastructure; and managing the DOE cybersecurity environment.

The Deputy CIO for Cybersecurity leads the Office responsible for OCIO's cybersecurity program, known within the Department as "IM-30." The IM-30 Office is further divided into three divisions. The first division, "Strategy and Policy," conducts work aligning to NIST's Identify element. Efforts aligned to NIST's Protect element are managed by the second division, "Cyber Implementation and Testing." The third division, "Cyber Operations," coordinate the Detect, Respond, and Recover elements of NIST's framework.

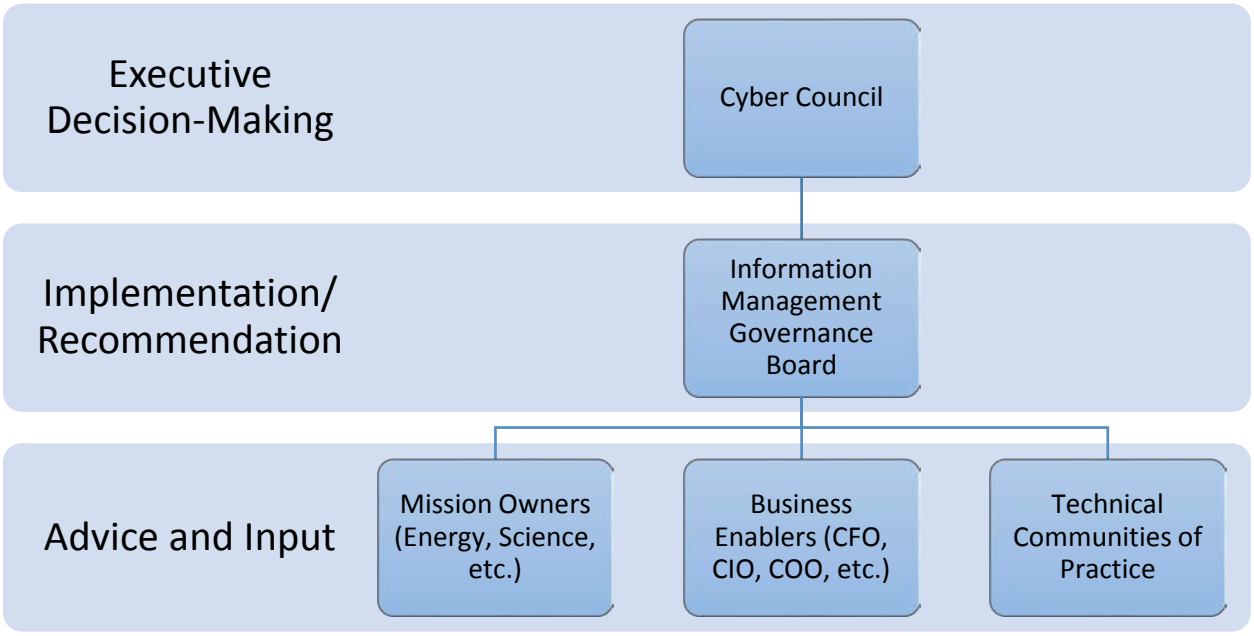
IM-30
Office of the Deputy CIO and
Chief Information Security Officer (CISO)

IM-31 **Strategy and Policy**	**IM-32** **Cyber Implementation & Testing**	**IM-33** **Cybersecurity Operation (iJC3)**
Strategy • DOE Cyber Strategy and Program • Security Plan Management • Contingency Planning • Policies, Waivers and Exceptions • Committee for National Security Systems (CNSS)	**Implementation** • DOE System Authorization • Enterprise Authority to Operate (eATO) • ATO Repository • Federal Risk and Authorization Management Program (FedRAMP) Support	**iJC3 Operations** • Enterprise Incident Response • Enterprise Information Sharing • Cooperative Protection Program (CPP) • Cyber Fed Model (CFM) • Automated Indicator Sharing (AIS)
Training and Awareness • Security Awareness Training	**System Testing** • EITS ATO Support • Independent Security Assessment • Periodic Testing • Plan of Action & Milestone (POAM) Management	**Cyber Assessments** • HVA Program • Cyber Risk Assessments
Outreach • FISMA • Legal and Regulatory Reporting		**Risk Management** • HVA Program • eSCRM
Plan **Identify**	Build **Protect**	Run **Detect, Respond, Recover**

Note: Blue Text indicates a FISMA 2014 Cybersecurity Program Requirement for a Federal Agency or Department

Support Services
- Data Collection
- Reporting
- Correspondence
- Budget and Finance Coordination

Appendix F: Extended DOE Cybersecurity Program Office



Strong cybersecurity governance and oversight assures that DOE is making the most of its cybersecurity budget to deliver a robust, secure set of tools.

Cyber Council

The DOE Cyber Council is the principal forum for collaboration and coordination of cybersecurity activities across the DOE Enterprise. The members of the Council include the Deputy Secretary (Chair), Associate Deputy Secretary, CIO, and other undersecretaries, directors, and leadership of the Department. The Council's focus is on the broad sphere of cyber, including information sharing and information safeguarding. The DOE Cyber Council's responsibilities include:

- Serving as the collaborative decision-recommending body for DOE Enterprise-wide cyber issues;
- Exercising oversight of the Cyber Governance Framework, including the Information Management Governance Board (IMGB) and its sub-groups, to support effective, efficient, and secure accomplishment of the Department's mission;
- Ensuring that the diverse array of mission perspectives are heard and, when consensus cannot be reached, document dissenting opinion(s) in relevant papers; and
- Resolving policy conflicts elevated by lower-level bodies.

Information Management Governance Board (IMGB)

While the Cyber Council governs Departmental cybersecurity policy, day-to-day implementation of that policy is coordinated by the Information Management Governance Board (IMGB). IMGB ensures that DOE has efficient IT project management and oversight. The IMGB uses mature project management processes to gain efficiencies and improve customer and stakeholder engagement across the enterprise. Effective IT governance empowers program offices to make decisions about their IT requirements, while providing guidance and support to ensure their success. In addition to implementing Cyber Council's policies, IMGB also makes recommendations to the Cyber Council for consideration and approval.

The Federal IT Acquisition Reform Act (FITARA) sets forth DOE CIO responsibilities relating to IT spending across the enterprise. This means that IT procurements will be centrally tracked and approved to reduce redundancies and ensure that security, monitoring, and overall integrity are core tenets of all IT purchases. The IMGB process is an integral piece of the DOE governance model and enterprise architecture and contributes to the effectiveness of that model.

Appendix G: FY18 to FY19 Performance Plan

Objective	#	Performance Goal (Measure)	Endpoint Target	FY2018 - Target	FY2019 - Target
2.1 IDENTIFY – **Enhance organizational capabilities to manage the cybersecurity risk.**	A	Hardware Asset Management - Achieve performance of 95% or greater for both Hardware Asset Management metrics (asset detection and asset meta data collection)	Annually maintain performance of at least 95% for both Hardware Asset Management metrics by FY 2018 and maintain annually thereafter.	≥ 95 %	≥ 95 %
	B	Software Asset Management - Achieve performance of greater than or equal to 95% for both Software Asset Management metrics (software inventory and software white-listing)	Obtain performance of at least 95% for both Software Asset Management metrics by FY 2018 and maintain annually thereafter.	≥ 95 %	≥ 95 %
2.2 PROTECT – **Develop and implement enterprise controls to reduce risk and increase resilience; promote enterprise cybersecurity awareness through workforce development and training.**	A	Federated Identity Management Infrastructure - Implement Federated Identity Management Infrastructure linking identity sources across DOE to OneID	Obtain performance of at least 95% of all identity sources across DOE linked to OneID by FY 2018 and maintain annually thereafter.	95%	95%
	B	High-Priority Application Authentication - Conduct a role-based risk assessment for all applications supporting high priority (FISMA) systems, identify the proper credential for each role within the application in accordance with the revised NIST 800-63 standard, and require the use of the proper credential for role-based access to the application.	Require the credential identified through the role based risk assessment for 80% of all applications supporting FISMA systems by FY 2021 and maintain annually thereafter.	30%	50%
	C	MFA - Privileged Network Account performance - Privileged Network Accounts that use a PIV credential or other NIST 800-63 r3 IAL3/AAL3/FAL3 must be equal to 100%.	Achieve an LOA4 performance of 100% for Privileged Network Accounts by FY 2018 and maintain annually thereafter.	100%	100%
	D	MFA - Unprivileged Network Account performance - Unprivileged Network Accounts that use a PIV credential or other NIST 800-63 r3 IAL3/AAL3/FAL3 must be equal to 85%.	Achieve an LOA4 performance of 85% for Unprivileged Network Accounts by FY 2018 and maintain annually thereafter.	85%	85%
	E	Secure Configuration Management - Achieve performance of greater than or equal to 95% for Secure Configuration Management	Obtain performance of at least 95% for Secure Configuration Management by FY 2018 and maintain annually thereafter.	≥ 95 %	≥ 95 %
	F	Standards Based Federated Access Management Infrastructure - Implement Standards Based Federated Access Management Infrastructure across DOE to enable single sign-on	Implement Standards Based Federated Access Management across 95% of DOE by FY 2018 and maintain annually thereafter.	95%	95%
	G	Vulnerability Management - Achieve performance greater than or equal to 95% for the detection of hardware and software vulnerability and weakness management	Obtain performance of at least 95% for Vulnerability Management by FY 2018 and maintain annually thereafter.	≥ 95 %	≥ 95 %

Objective	#	Performance Goal (Measure)	Endpoint Target	FY2018 - Target	FY2019 - Target
2.3 DETECT – **Develop tools and processes to accelerate notification of cybersecurity threats.**	A	Anti-Phishing - Performance of Anti-Phishing measurements must be greater than or equal to 90% on at least 5 of 7 capabilities.	Obtain performance of at least 5 of 7 anti-phishing capabilities at 90% or greater in FY 2017 and maintain annually thereafter.	≥ 5 capabilities greater than 90%	≥ 5 capabilities greater than 90%
	B	Malware Defense - Performance of malware defense measurements must be greater than or equal to 90% on at least 3 of 5 capabilities.	Obtain a performance of at least 3 of 5 malware defense capabilities at 90% or greater in FY 2017 and maintain annually thereafter.	≥ 3 capabilities greater than 90%	≥ 3 capabilities greater than 90%
	C	Other Defenses - Performance of "Other Defenses" measurements to include specific Anti-Phishing and Malware capabilities must be greater than or equal to 90% on at least 2 of 4 capabilities.	Obtain a performance of at least 2 of 4 other defense capabilities at 90% or greater in FY 2017 and maintain annually thereafter.	≥ 2 capabilities greater than 90%	≥ 2 capabilities greater than 90%
3.1 Customer Focused Cybersecurity	A	Migration of HQ analog phone customers to VoIP and decommission the HQ legacy analog phone switch.	Complete the migration of by the end of FY2018	100% Complete	N/A
	B	DOE HQ Network Refresh	Complete the Refresh (End of Life/Capacity) by the end of Q1 FY 2019	75% Complete	100% Complete
	C	Upgrade DOE HQ National Capital Region Network	Complete the Network Upgrade by the end of Q3 FY2018	100% Complete	N/A
	D	Enterprise Infrastructure-as-a-Service (IaaS) capabilities	Establish the initial enterprise IaaS capabilities by the end of Q3 FY 2018.	100% Complete	N/A
	E	Digital Transformation work streams initiatives	Complete the identified future modernization recommendations by the end of Q3 FY2018.	100% Complete	N/A
4.1 Risk Based Approach	A	Enterprise-level situational awareness of Cybersecurity Framework functions and key network activity	Provide enterprise-level situational awareness of Cybersecurity Framework functions and key network activity by end of FY 2019	50% Complete	100% Complete
	B	Enterprise Risk Management for Cybersecurity (ERM-CS) process flow and associated governance	Develop a concept of operations to describe the Enterprise Risk Management for Cybersecurity (ERM-CS) process flow and associated governance by end of FY 2019	50% Complete	100% Complete
	C	Strengthen enterprise IT risk management. through implementation of standardized IT cybersecurity requirements applicable across DOE established in an update to DOE IT Risk Management Framework and implementing it across Department elements	By FY 2019 implement of standardized IT cybersecurity requirements applicable across DOE established in an update to DOE IT Risk Management Framework and implementing it across Department elements	30% Complete	100% Complete
	D	Implement an Enterprise Architecture	By FY 2018 Implement Enterprise Architecture to standardize IT approaches in alignment with mission essential functions, reduce technical risks, and thereby increase cybersecurity	100% Complete	N/A

Appendix H: FISMA Cross Agency Priority Goal Targets

Summary of FISMA CAP Goal Targets & Methodology					
Capability	Target %	Agency Calculation	DOE FY18 (Q1)	DOE FY19 Target	Related DOE Cybersecurity Goal & Objective & Major Task From Implementation Plan
Information Security Continuous Monitoring (ISCM)					
▪ Software Asset Management	≥ 95%	95% Implementation	73%	85%	Goal 2 - Objective 1 – Major Task a
▪ Hardware Asset Management	≥ 95%	95% Implementation	90%	93%	Goal 2 - Objective 1 – Major Task a
▪ Authorization Management	100%	100% of High Impact Systems Authorized and 100% of Moderate Impact Systems Authorized	97%	98%	Goal 2 - Objective 1 – Major Task a.2
▪ Mobile Device Management	95%	95% Implementation	99%	99%	Goal 2 - Objective 2 – Major Task b
Identity, Credential, and Access Management (ICAM)					
▪ Privileged Network Access Management	100%	100% Implementation	96%	98%	Goal 2 - Objective 2 – Major Task b
▪ HVA System Access Management	≥ 90%	90% Implementation	89%	90%	Goal 1 - Objective 1 – Major Task c Goal 2 - Objective 1 – Major Task a.3 Goal 2 - Objective 2 – Major Task b
▪ Automated Access Management	≥ 95%	95% Implementation	47%	70%	Goal 2 - Objective 2 – Major Task b
Advanced Network and Data Protections (ANDP)					
▪ Intrusion Detection and Prevention	≥ 90%	At least 4 of 6 other metrics have met an implementation target of at least 90%	3	4	Goal 2 - Objective 3 – Major Task c
▪ Exfiltration and Enhanced Defenses	≥ 90%	At least 3 of 4 metrics have met an implementation target of at least 90%	2	3	Goal 2 - Objective 3 – Major Task a Goal 2 - Objective 3 – Major Task b
▪ Data Protection	≥ 90%	At least 5 of 7 metrics have met an implementation target of at least 90%	1	3	Goal 2 - Objective 2 – Major Task a - f

Appendix I: Key Challenges

1. **Cybersecurity Preparedness –**

- ***Increasing sophistication and frequency of cyber threats on a growing attack surface.*** The network environment has grown with the increased deployment of new digital devices (e.g. the internet of things (IOT)) that are located outside the physical boundary the department. These devices potentially introduce a greater variety of cyber-attack vectors. Monitoring capabilities of the critical data streams and communications pathways in networks must be bolstered to identify and ultimately disrupt emerging cyber-attacks.
- ***Meeting stringent privacy and security requirements while exchanging data*** **-** Real-time threat monitoring and analysis often requires exchanging sensitive data from operating environments, triggering privacy and liability concerns. Real-time threat monitoring requires technical products and assessments that meet the requirements of systems and ensure protection of sensitive data.
- ***Effective assessments require specialized expertise*** **-** Effective assessment of cybersecurity risks and capabilities requires consistent, industry-accepted tools and best practices. Departmental Element sites, particularly smaller sites may lack the skills and resources on staff to conduct assessments and prioritize mitigations without tools and resources.
- ***Information-sharing platforms require wide adoption to be most effective*** **-** Industry tools that share near- real-time threat indicators and threat analysis require wide testing with large- scale adoption to achieve their full value. Limited pilot implementations are insufficient to make a large impact on security or to effectively validate new tools.
- ***Information sharing requires processes in place prior to the threat*** **-** Vital information concerning high-level cybersecurity threats and risks is often classified. This makes it difficult to distribute the information widely if partners lack clearances and if information sharing processes are not in place prior to an event or threat. More efficient processes are needed to identify and prioritize private-industry partners who have a “need to know” and grant them appropriate security clearances.

2. **Incident Response and Recovery**

- ***Coordinating roles among many diverse stakeholders*** **-** Federal support of cybersecurity and incident response cuts across multiple government agencies and disciplines, from intelligence, to law enforcement, to emergency response. National leadership is needed to avoid issues such as conflicting roles and responsibilities and activities that are redundant or poorly aligned.
- ***Developing flexible, adaptable procedures*** **-** Cyber threats evolve quickly, and government hierarchies may not be well-suited for a rapid reprioritization of activities. Continuous coordination across the Federal Government is required to unify national efforts and limit the strain on the private sector of partnering with multiple departments and agencies.
- ***Coordinating geographically dispersed and diverse functional resources*** **-** Unlike many physical events, cyber events may affect infrastructure across a wide geographic area, and the consequences of an incident may be different for each affected system. Cyber incident response also may require a different set of resources, personnel, and skills than traditional energy disruptions. Some of these skills may not be included in traditional incident response procedures and training and may not be frequently tested.

3. Resilient Systems

- ***New solutions must support the business case -*** Develop cybersecurity tools and technologies that are economical, cost effective, and support operations, effectively making the system easier and less expensive to operate.
- ***Diverse legacy and modern devices -*** Cybersecurity solutions must integrate with existing systems that often contain a mix of new and legacy devices, a mix of platforms and vendors, and devices with different levels of computational and communications resources available to support cybersecurity measures.
- ***Solutions from diverse vendors and third-party providers must interoperate -*** New tools and technologies must be built to common standards to allow devices from different vendors to connect and operate without issue. Interoperable cybersecurity solutions require common standards development.
- ***Securing devices sourced from a global supply chain -*** Departmental Elements must ensure the integrity of the system hardware, firmware, and software components as they traverse the supply chain.
- ***Anticipating security in the future grid -*** Designing future systems with built-in cyber resilience requires anticipating future cyber threat scenarios and protection requirements.
- ***Meeting the growing demand for cybersecurity professionals -*** To manage and defend increasingly complex and sophisticated cyber systems, universities must build the nation's cybersecurity workforce. The current workforce increasingly faces heavy workloads, a shortage of critical skills, and constantly evolving expertise needs.

Appendix J: Acronyms

A&A	Authorization and Assessment
AAL	Authenticator Assurance Level
AIS	Automated Indicator Sharing
ANDP	Advanced Network and Data Protections
ATO	Authority to Operate
CAP	Cross Agency Priority
CATT	Cyber Analytics Tools and Techniques
CDM	Continuous Diagnostics and Mitigation
CESER	Cybersecurity, Energy Security and Emergency Response
CFM	Cyber Federated Model
CFO	Chief Financial Officer
CIO	Chief Information Officer
CNSS	Committee for National Security Systems
COO	Chief Operating Officer
COOP	Continuity of Operations Program
CPP	Cooperative Protection Program
CRISP	Cybersecurity Risk Information Sharing Program
CSF	Cybersecurity Framework
CSIP	Cybersecurity Strategy Implementation Plan
CYOTE	Cybersecurity for the OT Environment
DaaS	Desktop as a Service
DHS	Department of Homeland Security
DOE	Department of Energy
DRP	Disaster Recovery Plan
eATO	Enterprise Authority to Operate
E-ISAC	Electricity Information Sharing and Analysis Center
EITS	Energy IT Services
EO	Executive Order
ERM-CS	Enterprise Risk Management – Cybersecurity
eSCRM	Enterprise Supply Chain Risk Management
FAL	Federation Assurance Level
FCD	Federal Continuity Directive
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FISMA	Federal Information System Modernization Act
FITARA	Federal IT Acquisition Reform Act
GAO	Government Accountability Office
GFE	Government Furnished Equipment
HVA	High Value Assets
IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
ICT	Information and Communication Technology
iJC3	Integrated Joint Cybersecurity Coordination Center
IMGB	Information Management Governance Board

IN	Intelligence and Counterintelligence
IOT	Internet of Things
IS&S	Information Sharing and Safeguarding
ISCM	Information Security Continuous Monitoring
IT	Information Technology
MEF	Mission Essential Function
NCCIC	National Cybersecurity and Communications Integration Center
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NPPD	National Protection and Programs Directorate
NSS	National Security System
OA	Ongoing Authorization
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management & Budget
OT	Operational Technology
PCAP	Pack Capture
PIV	Personal Identity Verification
PMA	Power Marketing Administration
POAM	Plan of Action & Milestones
PPBE	Planning, Programming Budget and Execution
PPD	Presidential Policy Directive
RD&D	Research, Development, and Demonstration
SCRM	Supply Chain Risk Management
SOC	Security Operations Center
SP	Special Publication
TTX	Test, Training, and Exercise
UCS	Unified Coordination Structure
US	United States
US-CERT	United States Computer Emergency Readiness Team
WAN	Wide Area Network