U.S. Department of Energy

INFORMATION RESOURCES MANAGEMENT STRATEGY

FY 2018 – 2022

TABLE OF CONTENTS

A Message from the Deputy Secretary

Securing and managing the Department of Energy's information resources is crucial to the success of our diverse and vital missions. Across our enterprise, our National Laboratories, Power Marketing Administrations, plants, and sites rely on the safety, confidentiality, integrity, and availability of our information systems. This ***DOE Information Resources Management (IRM) Strategy*** sets out the path for the Department to approach the necessary solutions from an enterprise perspective: how we will improve our service delivery methods, modernize our technology, implement a new paradigm for how we acquire and manage IT solutions, and enhance our commitment to being good stewards of taxpayer dollars.

The Strategic Goals identified in this IRM are:

- Enhance Service Delivery for DOE Stakeholders
- Improve Information Technology and Cybersecurity
- Transition from IT Owner to IT Broker
- Excel as Stewards of Taxpayer Dollars

This IRM Strategy is the result of an enterprise-wide effort to determine how the Department can best align its information management efforts with key Federal legislation and guidance, such as the President's Management Agenda, the IT Modernization Report, the Modernizing Government Technology Act, and the 21st Century Integrated Digital Experience Act.

Central to the Department's efforts to properly manage our information resources is our comprehensive effort to implement an enterprise risk management framework across the DOE complex. By implementing enterprise risk management and shifting away from the old paradigm of compliance, DOE will be more able to respond to and recover from incidents quickly, and reassign Departmental resources to better mitigate risks.

The strategic goals and objectives identified in this document will enable the DOE workforce to modernize and improve the methods we use to execute our vital and diverse missions across the enterprise, while maintaining the highest standards of public service and stewardship of taxpayer resources.

I urge every Departmental element across the DOE enterprise, including the National Laboratories, Power Marketing Administrations, plants, and sites, to align all ongoing and future information resources initiatives to this IRM to the maximum extent possible.

I am pleased to endorse this Information Resources Management Strategy of the Department of Energy for 2018-2022.

Dan Brouillette
Deputy Secretary of Energy
May 2019

A Message from the Chief Information Officer

The U.S. Department of Energy's Office of the Chief Information Officer has prepared this Information Resources Management (IRM) Strategy to enhance and modernize the information resources and tools that the workforce of the Department uses to carry out our varied and unique missions. At the direction of Departmental leadership, the IRM was designed in collaboration with representatives from across DOE enterprise, and it was crafted from an enterprise perspective to ensure we will continue to work toward these strategic goals across our entire mission space.

This IRM identifies four key strategic goals that will guide our efforts to improve the delivery of services to our stakeholders and users, improve our IT and cybersecurity, change the paradigm for how we deploy IT solutions across the Department by shifting our role from IT owner to IT broker, and commit ourselves to continuing to be good stewards of taxpayer dollars.

In support of these goals, the IRM identifies a range of key objectives DOE will work to achieve between now and 2022, including:

- Create new capacity through the use of emerging cloud-based technologies that will achieve enhanced performance of information and IT services
- Adopt innovative cybersecurity technologies that support IT modernization and enable increased visibility and access to DOE cybersecurity posture
- Establish a best-in-class Enterprise Risk Management for Cybersecurity (ERM-CS) program to measure and manage cyber risk
- Improve interoperability and informed decision-making by developing formalized Departmental enterprise architecture, policy, processes, and standards
- Modernize the Department's Federal records and information management approach to achieve electronic records management to the fullest extent possible
- Seek to consolidate requirements to achieve economy-of-scale cost reductions, both inter-departmentally and intra-departmentally

The DOE IRM sets a path toward addressing a range of information resources challenges that we face as we transition the Department from legacy systems that allow vulnerabilities and unnecessary complexities to persist. Those legacy systems also fail to provide the new, modern tools necessary to adapt to the changing landscape of IT and cybersecurity that will pose new risks as we look to maintain and protect the safety, confidentiality, integrity, and availability of our information systems.

I am pleased to present the Information Resources Management Strategy for the Department of Energy for 2018-2022.

Max Everett
Chief Information Officer
U.S. Department of Energy
May 2019

BACKGROUND

INTRODUCTION

The Department of Energy (DOE) is committed to enhancing U.S. security and economic growth through transformative science, technology innovation, and market solutions to meet our energy, nuclear security, and environmental challenges. DOE's efforts are focused on modernizing the department's Information Technology (IT) and cybersecurity (cyber) infrastructure to deliver high quality IT and cybersecurity solutions, providing exemplary service to stakeholders and users, and excelling as stewards of taxpayer dollars. It is a requirement of all Federal agencies to establish a comprehensive approach to improve the acquisition and management of their information resources. This Information Resources Management (IRM) Strategy fulfills that task and will guide the direction, focus, mission alignment, principles, investments, and accountability of DOE's IT infrastructure.

DOE recognizes the importance of maximizing the quality and security of information systems, and developing and implementing uniform and consistent information resources management policies in order to inform the public and improve the productivity, efficiency, and effectiveness of agency programs. Additionally, as technology evolves, it is important that the Department manages information systems in a way that addresses and mitigates security and privacy risks associated with new information technologies, and new information processing capabilities. As specified by law, regulation, and various Office of Management and Budget (OMB) circulars and guidance memoranda, the Federal mandates require DOE to develop a plan that improves the procurement and management of its information resources.

Scope

DOE's IRM Strategy was developed leveraging enterprise-wide data inputs as both the drivers of the approach and to articulate the strategic direction. This IRM Strategy demonstrates how DOE does the following:

- **Advances** cybersecurity and the protection of information and information assets as core priorities across the enterprise
- **Protects** our information resources with adherence to Federal privacy and records management best practices
- **Implements** an IT and cybersecurity investment management process that links to and supports budget formulation and execution
- **Rethinks** and restructures the way work is performed before investing in new information systems
- **Manages** IT infrastructure modernization by developing data-driven and collaborative processes that maximize efficiency, flexibility, and security
- **Recruits, retains, retrains, and supports** a cybersecurity and IT workforce with the most current skills to meet enterprise needs
- **Delivers** innovative architecture, engineering, program, and product management with quality service to stakeholders and users, which will drive the continued success the DOE mission

Audience

The target audience for this IRM Strategy is DOE's enterprise, which includes program offices, independent DOE administrations, staff offices, National Laboratories, four Power Marketing Administrations, plants, and field sites across the country. This Plan will also provide information to partners across the executive and legislative branches of government, as well as the general public.

Alignment to DOE Mission and Federal Guidance

This IRM Strategy is aligned with DOE's mission and strategic planning to ensure America's security and prosperity by addressing its energy, environmental, and nuclear challenges through transformative science and technology solutions. This IRM Strategy also aligns with key Federal laws and guidance, including the Modernizing Government Technology (MGT) Act, the Federal IT Acquisition Reform Act (FITARA), the 21st Century Integrated Digital Experience (IDEA) Act, the Federal Information Security Modernization Act (FISMA), the Federal Records Act (FRA), the Privacy Act, and the President's Management Agenda.

Goals and Objectives

DOE's IRM Strategy is a comprehensive plan guided by four overarching, outcome-based goals, each of which is supported by multiple objectives. These IRM Strategic Goals will align DOE's information resources with DOE's mission to make information and IT solutions more efficient, useful, responsive, and accessible to all stakeholders and users.

Overview

GOAL 1 — Enhance Service Delivery for DOE Stakeholders

Objective 1.1
Better understand stakeholder requirements, preferences, and behaviors to improve enterprise information delivery and IT services

Objective 1.2
Create new capacity through the use of emerging cloud-based technologies that will achieve enhanced performance of information and IT services

Objective 1.3
Enable timely, evidence-based, and data-driven decision making through strengthened corporate data and information management processes to improve information availability and accessibility

Objective 1.4
Build a capability to sustain continual refresh of IT solutions through the deployment of IT innovations and enhancement of existing technologies

GOAL 2 — Improve Cybersecurity for Our Stakeholders

Objective 2.1
Adopt innovative cybersecurity technologies that support IT modernization and enable increased visibility and access to DOE cybersecurity posture

Objective 2.2
Establish a best-in-class Enterprise Risk Management for Cybersecurity (ERM-CS) program to measure and manage cyber risk by blending quantitative and qualitative frameworks that enable informed decision making

Objective 2.3
Foster a stronger sense of collaboration by establishing a community of interest made up of DOE and Federal cybersecurity professionals to support improved cybersecurity training and communication across the Department

GOAL 3 — Transition from IT Owner to IT Broker

Objective 3.1
Formalize organization structure, roles and responsibilities, rules of engagement and key processes

Objective 3.2
Determine optimum service delivery mix of personnel with associated skill sets to broker and manage services and then begin the transition to the "broker model" future state

Objective 3.3
Hire and contract professionals skilled in best-in-class practices who will promote and improve stakeholder and user satisfaction. Retrain existing personnel as part of our talent management process

Objective 3.4
Promote an enterprise approach to services management that will foster innovation by collaborating with government, industry, and academic partners

GOAL 4 — Excel as Stewards of Taxpayer Dollars

Objective 4.1
Improve interoperability and informed decision-making by developing formalized Departmental enterprise architecture, policy, processes, and standards

Objective 4.2
Improve Departmental decision-making by improving and formalizing governance processes based upon prioritized user requirements and a risk-based approach.

Objective 4.3
Increase the efficiency of Department IT investments by streamlining IT acquisition, improving project management processes, increasing cost transparency, and formalizing FITARA expectations

Objective 4.4
Seek to consolidate requirements to achieve economy-of-scale cost reductions, both inter-departmentally and intra-departmentally

Objective 4.5
Modernize the Department's Federal records and information management approach to achieve electronic records management to the fullest extent possible

GOAL 1

ENHANCE SERVICE DELIVERY FOR DOE STAKEHOLDERS

IT and cybersecurity are integral to DOE's daily operations. DOE remains committed to providing excellent services to our stakeholders and ensuring high levels of user satisfaction. Supporting the stakeholders whose missions depend on these services is a top priority for the Department. DOE will continue to strengthen its relationships with its stakeholders and users to better understand their business requirements and deploy modern and secure solutions to enable their missions, and provide greater usability of services. Greater understanding of user requirements will allow for tailored and flexible delivery of IT and cybersecurity solutions that will drive successful mission outcomes. To improve service delivery, DOE will continue to modernize its information ecosystem, enhance existing solutions, and provide new and emerging solutions based on evolving technologies and cloud services to deliver maximum value to its consumers, enabled by the new emerging and advanced solutions division.

OBJECTIVES

1.1 BETTER UNDERSTAND STAKEHOLDER REQUIREMENTS, PREFERENCES, AND BEHAVIORS TO IMPROVE ENTERPRISE INFORMATION DELIVERY AND IT SERVICES

Stakeholder engagement is a core element of delivering improved services and solutions to users. DOE will continue to innovate by enhancing our understanding of users' business requirements and work processes to better leverage existing enterprise services and anticipate users' future IT service needs across the wide range of unique mission areas throughout the enterprise. The effort will use approaches like journey mapping, user/human-centered design, and agile business architecture to develop a deeper knowledge base. In addition, targeted and continuous user feedback and performance measures will drive more rapid and secure deployments of IT solutions to enable business and mission outcomes, while providing greater usability.

1.2 CREATE NEW CAPACITY THROUGH THE USE OF EMERGING CLOUD-BASED TECHNOLOGIES THAT WILL ACHIEVE ENHANCED PERFORMANCE OF INFORMATION AND IT SERVICES

DOE remains focused on acquiring and deploying solutions to improve enterprise cybersecurity, scale capacity commensurate with demand, and establishing enterprise capabilities that allow for the implementation and the enhancement of IT services. Continuing the IT service modernization efforts that the Energy Information Technology Services organization began in FY 2018, DOE will transition current IT Services to managed and cloud services, and establish new capabilities and capacity by deploying emerging technologies to mitigate dynamic and evolving risks. As technologies and workforce mobility increase, DOE will continue to explore the "office of the future" concept by enhancing mobility and desktop services to support the "anytime, anywhere" paradigm of the modern workforce.

An example of these efforts is DOE's work on its Headquarters transition to Voice-over-IP (VoIP) services, and its work to pilot the use of the Trusted Internet Connection (TIC) Overlay with Microsoft's Office 365 cloud services, which eliminates one of the significant obstacles to the Federal Government's move to cloud services. In addition, DOE has established cloud environments in Amazon AWS and Microsoft Azure, which offer engineered and inherent cybersecurity capabilities in support of the Data Center Modernization initiative to enhance the integrity, authenticity, and accuracy of the records and information maintained in those clouds. DOE continues to engage in efforts to modernize the TIC architecture in support of Federal mandates to reduce and consolidate external access points, enhance security requirements, improve the management of electronic Federal records while emphasizing privacy and data security, and increase security monitoring to protect our information assets.

1.3 Enable timely, evidence-based, and data-driven decision making through strengthened corporate data and information management processes to improve information availability and accessibility

The ability to collect, consume, manage, and share authentic, accurate, and trustworthy data is crucial to mission success, which is why building both a culture of, and a common approach to, data-driven decision-making and evidence-based policy is a priority across the Department. Departmental compliance processes implement the laws, regulations, policies, and Departmental orders that govern the handling of, safeguarding of, and access to information. DOE has established a Chief Data Officer to develop and execute the Department's Data Strategy to deliver and receive high-value data and information in an easily-discoverable, retrievable, and recordable format that promotes transparency and electronic records management. DOE's Chief Data Officer (CDO) is responsible for establishing a governance foundation for sharing data, along with policy that supports the Department's Data Strategy, including its efforts across geospatial science and artificial intelligence (AI). DOE's Data Strategy is representative of the artificial intelligence building block of the Department's Enterprise Architecture (EA) Framework, which is a blueprint for collaboration that defines value-centric Enterprise Architecture (an evolutionary asset and practice). The core of the EA Framework is the DOE mission, which consists of four main areas: Energy, Science & Innovation, Nuclear Safety & Security, and Management & Operational Excellence. The EA Framework promotes enterprise-wide synergy towards the creation of common business, data, and IT services and solutions, and enables safe and secure mission outcomes. It also ensures that communications and interactions are impactful and dynamic by creating a consistent and seamless experience of stakeholder engagement, with the goal of continually exceeding expectations. One way DOE is facilitating this is by periodically providing performance-to-cost documentation for services rendered, such as cost per person for desktop support, downtime, service calls, technician dispatches, and trouble ticket statistics. This promotes transparency in the total cost of services and fosters improved business partnerships to better understand user requirements and steer system enhancements to support them.

1.4 Build a capability to sustain continual refresh of IT solutions through the deployment of IT innovations and enhancement of existing technologies

DOE will continue to encourage the use of cloud and shared services and cloud solutions across the Department and with Federal agency partners, while developing appropriate service level agreements to ensure operational and mission requirements are met. DOE also continues to implement strong FITARA policies that encourage shared services and cloud solutions, as well as the adoption of agile project management methodologies. In alignment with OMB's Federal Cloud Smart Strategy, DOE will continue to mature the enterprise information ecosystem towards an architectural model that improves the

user experience. This is done by increasing user capacity, fostering flexibility and elasticity, reducing spending on redundant and static infrastructure and commodity services, and strengthening the security of information. The Department's Cloud Smart Reference Guide will continuously evolve, promoting the latest techniques and approaches to cloud planning and migrations that maximize investment returns. The increased use of shared and cloud services will enable the Department to rapidly deploy enhancements to existing services and utilize new and innovative services and solutions in a continuous improvement/continuous change lifecycle. An example of this is DOE's Data Center Modernization effort, discussed above, which established cloud environments in Amazon AWS and Microsoft Azure to provide flexible, integrated virtual data center capabilities. In alignment with the Federal Data Center Optimization Initiative (DCOI), this effort also focuses on migrating application workloads into these cloud environments, reducing and eventually eliminating the physical on premises infrastructure at the legacy Germantown and Albuquerque data centers. This provides DOE Headquarters and enterprise users with dynamic and on-demand capacity, addresses the current operational risks associated with the legacy data centers and aging infrastructure, and provides modernized and highly secure data center services that are essential to maintaining continuity of mission-critical services.

GOAL 2

IMPROVE CYBERSECURITY FOR OUR STAKEHOLDERS

DOE leverages and incorporates assets and capabilities from across all Departmental elements to protect the safety, confidentiality, integrity, and availability of information systems by continually improving the enterprise's cybersecurity posture while also protecting the privacy of individuals. One of the biggest challenges DOE faces due to the complexity of the enterprise and the diversity of its missions is gaining and maintaining comprehensive situational awareness to inform risk decisions, both for particular elements and the enterprise as a whole. Today's rapidly shifting cyber threat landscape has made improved situational awareness across the enterprise vital to protect against increasingly sophisticated adversaries who seek to exploit the diversity of DOE's mission space. The Department's enterprise risk management framework will provide a quantitative means by which to prioritize resources for risk mitigation rather than compliance. This will be a valuable tool for reducing costs and developing effective cybersecurity programs, while also aligning with a strong focus on privacy protection, including the safeguarding of personally identifiable information. Finally, we will build a community of interest comprised of cybersecurity professionals from across the DOE enterprise and the Federal Government to support the DOE cybersecurity workforce.

OBJECTIVES

2.1 ADOPT INNOVATIVE CYBERSECURITY TECHNOLOGIES THAT SUPPORT IT MODERNIZATION AND ENABLE INCREASED VISIBILITY AND ACCESS TO DOE CYBERSECURITY POSTURE

DOE remains focused on adopting innovative technologies in support of IT modernization. The Department is developing repeatable processes for clearly defining objectives and tracking/reporting compliance with Federal and Departmental direction, as well as leveraging Continuous Diagnostics and Mitigation (CDM) to reduce the manual Federal reporting burden, while improving risk management through increased visibility. Maturing the Integrated Joint Cybersecurity Coordination Center (iJC3) and site/lab security operations centers (SOCs) to ensure consistent detection and remediation of incidents, along with increasing the automation of information sharing, detection, and analysis are crucial to the success of this objective. Establishing a foundation for machine learning and AI will allow the Department to gain and leverage new insights that will rapidly advance a range of outcomes. For example, the Department will continue to implement its Big Data Platform (BDP) to provide a cloud-based, scalable analytics platform, which will enable enterprise monitoring, analysis, and reporting. BDP allows cybersecurity analysts to focus their efforts on higher-level analysis and the most urgent needs. BDP and similar efforts will ensure that DOE directs its resources and activities toward the highest-value systems and the most important risks.

2.2 ESTABLISH A BEST-IN-CLASS ENTERPRISE RISK MANAGEMENT FOR CYBERSECURITY (ERM-CS) PROGRAM TO MEASURE AND MANAGE CYBER RISK BY BLENDING QUANTITATIVE AND QUALITATIVE FRAMEWORKS THAT ENABLE INFORMED DECISION MAKING

DOE is establishing a best-in-class Enterprise Risk Management for Cybersecurity (ERM-CS) program to measure and manage cyber risk to enable Departmental leadership to make informed and cost-effective mission and business decisions. The DOE Cybersecurity Program approaches implementation of cybersecurity requirements in a manner commensurate with impact to mission, national security, risk, and magnitude of harm, while also addressing both IT and operational technology systems. The DOE Cybersecurity Program empowers Departmental elements by providing them with the flexibility to tailor and implement cybersecurity risk mitigation controls in consideration of threats, acceptable risks, and mission needs, as well as environmental and operational factors.

2.3 Foster a stronger sense of collaboration by establishing a community of interest made up of DOE and Federal cybersecurity professionals to support improved cybersecurity training and communication across the Department

DOE recognizes cybersecurity is a shared responsibility of the entire workforce. That's why it will further enable all DOE employees to meet the challenge of a shared cyber mission by clearly communicating risks and individual cybersecurity responsibilities. The Department will continue to provide enterprise options for training to support the continued learning and knowledge of our cybersecurity workforce. Another priority for the Department is conducting exercises with stakeholders to help them build competencies in and appreciate the challenges of cybersecurity risk management. Stakeholders are more engaged when they can see how risk management can have an impact on their individual contributions to achieving the DOE mission. This increased collaboration, awareness, and role-based training across the enterprise is essential to the Department's long-term success.

GOAL 3

TRANSITION FROM IT OWNER TO IT BROKER

Modernizing DOE's IT infrastructure involves recognizing the changing landscape of business priorities, which prompts the need to shift from operations to value creation. The transformation from IT owner to IT services broker is necessary to support this shift. The IT owner model inherently supports the status quo and prioritizes operations and maintenance (O&M) spending. IT owners are wedded to existing systems and programs; measure success at meeting user requirements that may be out of alignment with mission requirements; and promote a one-size-fits-all approach. In contrast, the IT service broker model structurally prioritizes spending on delivering value to users. IT service brokers focus on the outputs and capabilities required by users, not the systems that deliver those capabilities. IT service brokers measure success based on delivery of value on an ongoing basis, rather than against a historical checklist of requirements. This posture requires IT service brokers to utilize agile delivery techniques and structures. IT service brokers adapt services to user requirements and, where necessary, adapt existing services or develop new capabilities to meet mission needs. The IT service broker model will ensure the Department can maximize the value of managed services and cloud services. DOE continues to address organizational change and governance processes to more effectively transition to and operate as an IT services broker.

OBJECTIVES

3.1 FORMALIZE ORGANIZATION STRUCTURE, ROLES AND RESPONSIBILITIES, RULES OF ENGAGEMENT AND KEY PROCESSES

DOE will continue to address DOE's organizational change and governance processes to more effectively transition and operate as an IT services broker. It will produce a map for users, clients, and stakeholders that details jurisdiction, membership, points of contact, and relationships between the Department's IT and cybersecurity governance bodies. It will further establish centralized technical capabilities and optimize business and technology processes to effectively deliver new capabilities provided by commercial cloud and managed services.

3.2 DETERMINE OPTIMUM SERVICE DELIVERY MIX OF PERSONNEL WITH ASSOCIATED SKILL SETS TO BROKER AND MANAGE SERVICES AND THEN BEGIN THE TRANSITION TO THE "BROKER MODEL" FUTURE STATE

DOE's professional workforce continues to be our most important asset, and must always be given priority consideration during any problem-solving or decision-making process. User and stakeholder experiences are a central measurement for achieving meaningful impacts. Culture and human skills and knowledge must evolve as the Department progresses with automation and other aspects of digital transformation. To further align mission and business requirements with solutions, DOE will continue its transition to commercial cloud and managed services. Improving this service management requires DOE to continually identify future workforce requirements and skillset gaps, as well as ensuring the Department's entire operating model is aligned for optimized service delivery. This includes supporting DOE's cybersecurity and IT workforce to keep pace with continuous changes in an ever-evolving environment, as well as reskilling efforts to give employees new and current skills support growth and development while filling critical mission needs. Another priority for the Department is formalizing its stakeholder and user relationship management approach to allow for clearly-defined expectations for collaborations with IT brokers.

3.3 HIRE AND CONTRACT PROFESSIONALS SKILLED IN BEST-IN-CLASS PRACTICES WHO WILL PROMOTE AND IMPROVE STAKEHOLDER AND USER SATISFACTION. RETRAIN EXISTING PERSONNEL AS PART OF OUR TALENT MANAGEMENT PROCESS

The Department's goal of shifting from the traditional owner and operator of IT services to brokering and managing services provided by cloud and managed-service providers requires a significant change in workforce structure and skills. With the rapid pace of changing technology, a lifecycle management approach to technical skills and instilling

the value of technical and behavioral skill versatility is key for staff to be able to effectively manage services in this new paradigm. The Department recognizes the need to identify existing and future skill competency gaps, develop appropriate succession plans, and implement knowledge management solutions to mitigate the risk of DOE's retirement-eligible workforce, and standardize enterprise-wide training. Success of this objective also requires DOE to effectively leverage contractor partners with an inherent approach to continuous improvement of stakeholder and user engagement to deliver high quality services and solutions. In support of this, DOE has awarded a new IT Services contract, CIO Business Operations Support Services (CBOSS), which provides vendors with proven capabilities and experience in delivering excellent service to users and stakeholders. In working closely with the Chief Human Capital Office, DOE is committed to supporting the objective of developing a highly qualified, capable, and flexible Federal workforce.

3.4 Promote an enterprise approach to services management that will foster innovation by collaborating with government, industry, and academic partners

The Department partners closely with government, industry, and academic innovators to discover and deploy new technologies and share best practices. DOE will continue to establish new relationships and advance existing partnerships to promote information sharing and collaborative innovation. The Department will also continue to implement partner-established policies and standards, while continually engaging with innovators to learn about new technologies and business practices. The most promising innovations will be rigorously tested, and if found to be effective and feasible, the Department will incorporate them into the appropriate environments. Examples of DOE's efforts to foster intellectual exchange include the keynote lectures, symposia, and forums that DOE hosts across the enterprise to inform the workforce and highlight DOE's IT and cybersecurity efforts.

GOAL 4

EXCEL AS STEWARDS OF TAXPAYER DOLLARS

In its IT modernization efforts, DOE continues to refine its current IT governance practices to improve prioritization and identification of user-centric opportunities. This involves bolstering workforce training and development—as well as improving resources management—to reduce the time associated with data collection, management, and reporting. The Department will continue to seek opportunities to remove silos and fully interconnect the enterprise to strengthen the workforce's ability to collaborate seamlessly, resulting in maximized productivity and cost efficiency. In alignment with Federal mandates, DOE continues to prioritize transparency, accountability, and efficiency in its IT services delivery to further excel as stewards of taxpayer dollars.

OBJECTIVES

4.1 IMPROVE INTEROPERABILITY AND INFORMED DECISION-MAKING BY DEVELOPING FORMALIZED DEPARTMENTAL ENTERPRISE ARCHITECTURE, POLICY, PROCESSES, AND STANDARDS

DOE continues to establish and enhance policies and procedures supporting the efficient and effective collection of information, as well as provide relevant training and awareness to the Department's workforce. DOE also continues to evolve our Capital Planning and Investment Control process with the implementation of Technology Business Management (TBM) to enhance the transparency of costs and performance. With the implementation of TBM, DOE is also more closely linking IT Portfolio data with our Federal Information Technology Acquisition Reform Act (FITARA) budget planning and acquisition review processes to improve interoperability. This is linked with DOE's governance goals of providing strategic direction, ensuring that plans and objectives are achieved, assessing whether risks are actively managed, and assuring that key IT activities are coordinated. DOE will also continue to strengthen its electronic and paper records management capabilities, with a focus on achieving a fully electronic records management environment to the greatest extent possible.

4.2 IMPROVE DEPARTMENTAL DECISION-MAKING BY IMPROVING AND FORMALIZING GOVERNANCE PROCESSES BASED UPON PRIORITIZED USER REQUIREMENTS AND A RISK-BASED APPROACH

DOE uses a fully inclusive, transparent, and responsive IT and cyber governance approach to ensure the efficient and effective delivery of IT and cyber services and solutions through its IT investments. The Deputy Secretary chairs the DOE Cyber Council, and members include senior leaders from DOE Program Offices, National Laboratories, and Power Marketing Administrations, to develop a rigorous and collaborative approach to securely and efficiently managing enterprise-wide information resources. The CIO is a member of the Energy System Acquisition Advisory Board (ESAAB), the Secretarial-level review board for major system acquisitions in DOE. The CIO chairs the Information Management Governance Board that consists of senior officials from the DOE enterprise with responsibility for IT systems and cybersecurity, and serves as the forum for collaboration, development, coordination, and implementation of enterprise information resources management and cyber activities and issues. The CIO also continues to engage the National Labs in many ways, such as participating in annual lab planning meetings. The Department continues to emphasize IT performance reviews in the annual DOE Performance, Evaluations, and Measurement Plan (PEMP) process, which provides greater oversight by formally including the DOE CIO and CIOs from across the enterprise in the review process. DOE also continues to work to identify ways to refine the IT Portfolio reporting process, in order to capture

relevant performance data regarding Maintenance and Operations (M&O) spending across both mission and support IT, and also in both major and non-major investments.

4.3 Increase the efficiency of Department IT investments by streamlining IT acquisition, improving project management processes, increasing cost transparency, and formalizing FITARA expectations

IT budget formulation, governance, acquisition, and project management processes are essential to DOE. The Department continues to bring greater rigor to the budget formulation process and efficiencies to the IT acquisition development pipeline. DOE continues to conduct annual peer reviews of project and program requirements, and is working with the Department's Working Capital Fund and leadership to enable funding tools to manage the life cycle cost of IT solutions across the enterprise, in alignment with the MGT Act. Another priority is ensuring leadership buy-in for investments and projects, such as by identifying common IT issues and recommending resolutions to the Deputy Secretary of the Department. Through preparation and reporting of the Department's IT Budget, DOE ensures collaboration with the Office of the Chief Financial Officer and alignment with the Department's annual Budget Request. It remains a high-level DOE priority to have a mature acquisition review process, to empower CIOs to drive enterprise strategy and enforce IT policy via centralized software licensing. Also, as required by FITARA, DOE continues to promote CIO engagement in the performance management of the Department's IT Portfolio through participation in component-level Investment Review Boards (IRB) and the review of major investments by the DOE IRB. All of these activities work in combination to support the Department's life-cycle management approach for IT projects and operations.

4.4 Seek to consolidate requirements to achieve economy-of-scale cost reductions, both inter-departmentally and intra-departmentally

In November 2018, DOE awarded its new CBOSS blanket purchase agreement to provide cybersecurity, IT operations, telecommunications, and related IT support to DOE headquarters elements. The purchase agreement is also available for use by the DOE Power Marketing Administrations, sites, and National Laboratories. In addition to the critical mission support of providing the Department's IT services, the new contract will assist our IT modernization efforts in several ways, including transitioning the Department away from relying on legacy, internally-hosted IT, to becoming a service provider of innovative cloud-based shared services across the Department's diverse missions; enhancing the Department's cybersecurity posture; and consolidating IT services around the Department, thereby reducing administrative overhead. This is the beginning of a transformative shift, transitioning OCIO from IT owner to IT broker—one of our key strategic goals. This contract is also an important step toward improving how we work with our stakeholders and users, while being good stewards of taxpayer dollars. This contract will enable us to modernize not only our aging technology, but also

to improve our processes and operations across the DOE enterprise, especially in the critical area of cybersecurity.

DOE continues to increase its use of enterprise-wide agreements to consolidate and standardize software licensing products and take full advantage of economies of scale, while minimizing duplicative investments in existing security capabilities. This facilitates the adoption of shared and cloud services for non-mission specific functions, as well as Best-In-Class (BIC) contracts, commodity IT services and other collaboration productivity, and security tools. A Department-wide initiative exemplifying this is its effort in eliminating on-premises email systems with the migration to a Government Community Cloud service based upon Microsoft's Office 365 (O365). Moving to O365 allows DOE to scale messaging services to future changes in its user base without the need to accommodate large infrastructure investments; it also reduces support and maintenance staff. The end result for DOE is not only cost savings, but also a wealth of gained knowledge it can provide as shared lessons-learned and recommendations to other Federal agencies also seeking to migrate to the O365 cloud. DOE will also be initiating a multi-office project to design and implement a modernized network architecture for the DOEnet corporate business network, leveraging the existing Energy Sciences Network (ESnet) to address the Department's wide-area network transport requirements. Through a combination of increased use of shared services, targeted alignment of common IT services to a minimum number of providers, and federation of the enterprise operating environments, DOE continues striving to fully interconnect the enterprise in order to maximize our employees' ability to collaborate seamlessly across the DOE information ecosystem, in support of the Department's mission.

4.5 Modernize the Department's Federal records and information management approach to achieve electronic records management to the fullest extent possible

The Department is transitioning to fully-electronic recordkeeping in accordance with the objectives of the National Archives and Records Administration (NARA) 2018-2022 Strategic Plan, which includes, to the fullest extent possible, plans to no longer transfer permanent or temporary records in analog formats to NARA after 2022. The Department will transition its Federal recordkeeping to a fully-electronic environment in order to reduce costs and create efficiencies, while increasing appropriate and timely access to records and information. Included in this effort is an enterprise digital signature strategy and enterprise-level business process redesign, to ensure all Federal records and information processes are born digital and remain digital throughout the records lifecycle.