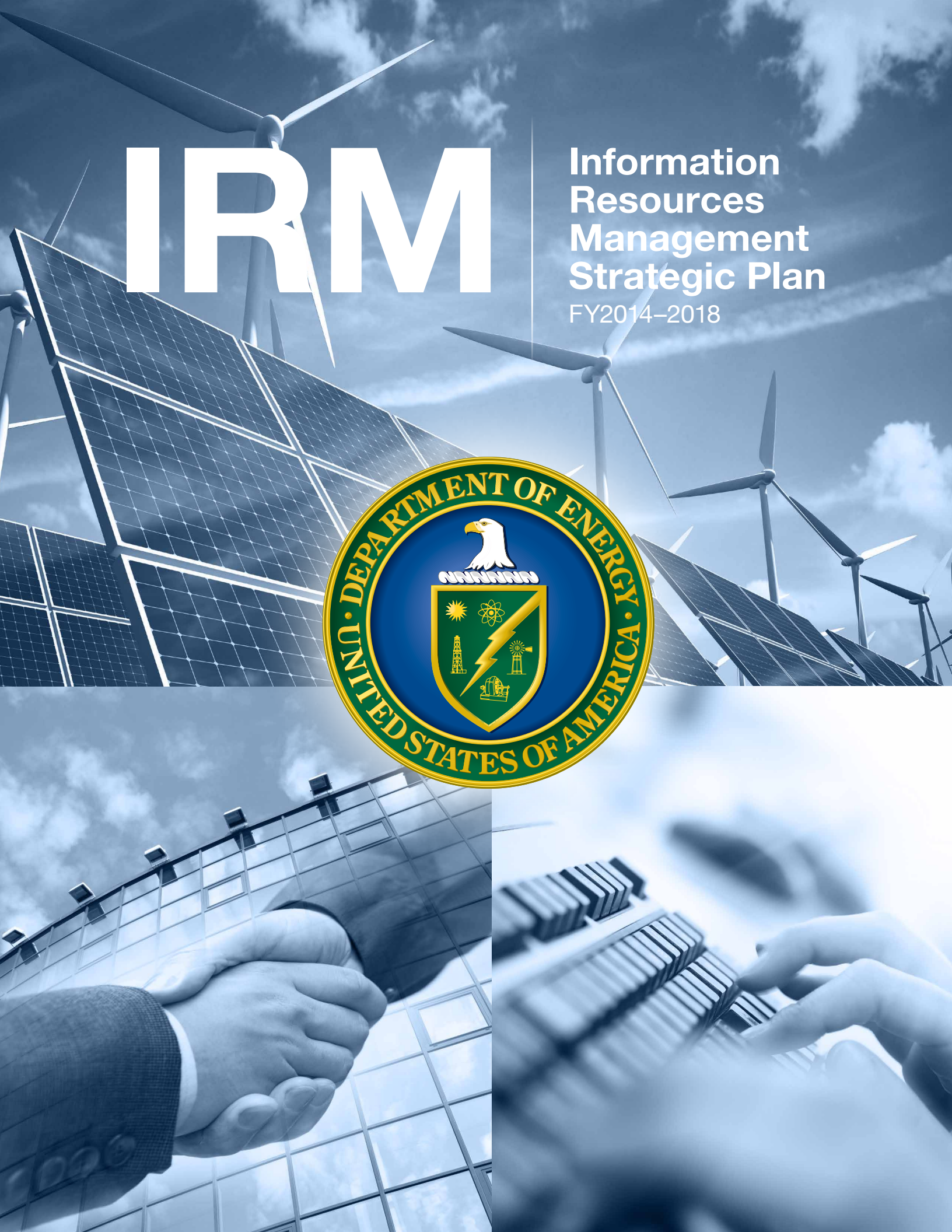


IRM

Information Resources Management Strategic Plan

FY2014–2018

DOE IRM Mission

Advance the Department's mission through policy, standards, and services, which meet mission requirements, balance risk and innovation, and set clear performance goals and expectations for the information ecosystem.

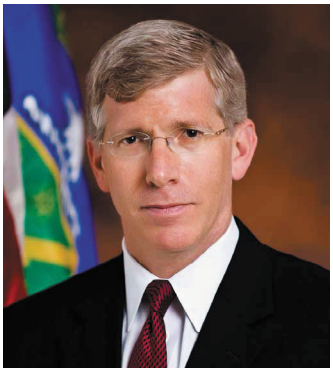
DOE IRM Vision

Collaborate as an enterprise to deliver innovative information management and technology solutions that support the Department's mission.

Core Capabilities

Governance • Information and IT Management • Enterprise Architecture, Policy, and Standards
Cybersecurity • IT Workforce Management

Strategic Goal 1	Strategic Goal 2	Strategic Goal 3	Strategic Goal 4
"Supporting our information consumers"	*"Excelling as stewards of enterprise IT resources"*	*"Enhancing information security"*	*"Investing in our workforce and partners"*
Ensure delivery of high-quality information and IT solutions that meet consumers' needs and enable mission outcomes.	Safeguard our resources through the cost-effective management of information and IT solutions.	Protect the integrity of Departmental information by strengthening our cybersecurity posture.	Invest in our IT workforce and the partnerships required to advance the Department's mission.
Objectives	**Objectives**	**Objectives**	**Objectives**
1.1 Improve delivery of enterprise information and IT solutions by understanding consumers' needs, preferences, and behaviors. 1.2 Create new capacity through a network of DOE clouds that will achieve enhanced performance of information and IT solutions by integrating networks and services. 1.3 Ensure the availability of and access to information that enables consumers to make timely, informed decisions by strengthening corporate data and information management approaches. 1.4 Provide IT solutions by deploying innovative information technologies while enhancing existing technologies.	2.1 Improve interoperability and compliance by enhancing Departmental enterprise architecture, policy, and standards. 2.2 Improve Departmental decision-making by strengthening governance processes. 2.3 Increase the efficiency of Department IT investments by streamlining IT acquisition and improving project management processes.	3.1 Fulfill Federal security requirements by establishing standards and expectations for Departmental cybersecurity. 3.2 Prevent and promptly resolve cybersecurity threats by strengthening Departmental situational awareness and incident response. 3.3 Develop and transition cutting-edge technologies into the DOE security architecture by advancing the Cyber Sciences Laboratory and the Cyber Innovation Center. 3.4 Promote enterprise cybersecurity awareness and foster a stronger sense of accountability by improving cybersecurity training and communication.	4.1 Support the Department's information technology needs by building a talented, diverse workforce. 4.2 Enable the IT workforce to execute its responsibilities by providing useful, secure technology and processes. 4.3 Promote an enterprise approach to information sharing that will foster innovation by collaborating with government, industry, and academic partners.



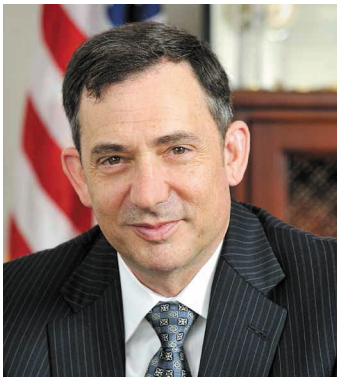
Daniel B. Poneman
Deputy Secretary of Energy

Message from the Deputy Secretary

The Department of Energy (DOE) has a rich history of enhancing U.S. security and economic growth through transformative science, technology innovation, and market solutions to meet our energy, nuclear security, and environmental challenges. The success of this mission is highly dependent on the quality, availability, and usability of information and Information Technology (IT). By optimizing information processes, services, and technology, we will be better positioned to deliver high-quality solutions, achieve cost-effectiveness, improve security, and enhance collaboration across the Department to enable the DOE mission.

The FY 2014-2018 DOE IRM Strategic Plan will guide the future of Departmental information and IT. Active participation and commitment will be required from all Departmental Elements to achieve its intended results. Now unified by a single IRM Strategic Plan, the Department will meet and exceed the rising expectations of our stakeholders, business partners, and the information consumers that we serve.

Daniel B. Poneman
Deputy Secretary of Energy



Robert F. Brese
Chief Information Officer

Message from the Chief Information Officer

I am proud to present the FY 2014-2018 DOE Information Resources Management (IRM) Strategic Plan, which defines the goals we — the DOE IT organizations — must meet, the capabilities we must build, and the strategies we must implement to support achievement of the DOE mission. Prior to the FY 2014-2018 DOE IRM Strategic Plan, the Department had more than 15 strategic documents that guided DOE information and IT efforts. By synthesizing and supplementing critically relevant concepts from these previous strategic documents, the DOE IRM Strategic Plan describes how we will align our information resources with the Department's mission to make information and IT solutions more efficient, useful, responsive, and accessible to all information consumers.

To realize our forward-leaning information and IT vision, we will continue to build upon the three pillars — *Transform, Protect, Advance* — established in the 2012 IT Modernization Strategy. Designed to be enduring, these three pillars describe the means by which we will accomplish our four IRM strategic goals. First, we must ensure the delivery of high-quality information and IT solutions that meet consumers' needs and enable mission outcomes. Second, we must safeguard our resources through the cost-effective management of information and IT solutions. Third, we must protect the integrity of Departmental information by strengthening our cybersecurity posture. Finally, we must invest in our IT workforce and collaborative partnerships. While we will face challenges over the next four years, through the IRM Strategic Plan we will continue to modernize the way we manage, use, and secure our information and IT to advance the Department's mission.

Robert F. Brese
Chief Information Officer

Table of Contents

Major Trends Affecting DOE Information and IT: FY 2014–2018

DOE enhances U.S. security and economic growth through transformative science, technology innovation, and market solutions to meet our energy, nuclear security, and environmental challenges. To advance this mission, it is paramount that DOE effectively and efficiently manage its enterprise information resources. In coming years, we anticipate that we will encounter several technological, policy, workforce, and economic challenges that will impact our operations. We will embrace these challenges as opportunities to improve operational efficiency, advance our cybersecurity defenses, and better serve the Department's mission. The DOE IRM Strategic Plan accounts for each of these trends as we plan our strategic priorities.

Evolving Complexity of the Department's Information Ecosystem

From the Energy Information Administration to the federally funded national laboratories, DOE is composed of drastically different Departmental Elements. (DEs). The Department has highly varied mission areas, resulting in a federated organizational structure. This structure has caused the way in which we manage and use information to become increasingly complex in recent years. For instance, within the Federal area alone, in Fiscal Year (FY) 2012, the DOE commodity IT environment included numerous IT Directors, hundreds of IT operations personnel, more than 20 email systems, and 46 data centers of varying size. Though the consumer base for each of these services varies, duplication of technology and support is common across our information ecosystem.[1] To begin addressing these specific instances of complexity, in FY13 the Secretary mandated a Departmental 120-day study to determine how DOE can deliver improved service of Federal IT with increased efficiency. Based on the resulting recommendations from this study, we will undertake initiatives to increase transparency and accountability across our IT portfolio, create consistent management frameworks that enable an appropriately standardized customer requirements process, and develop a more flexible enterprise architecture that will facilitate integration of future technology advances and enable the Department to provide consumers with the IT services they want. Ultimately, we will have a collection of systems that are seamlessly interoperable and secure across the Department, thereby optimizing the DOE information ecosystem.

In FY12, 12 different DOE Program and Staff Offices operated more than 120 instances of 26 DOE commodity IT services.

Growing Frequency and Sophistication of Cybersecurity Threats

Adversarial cybersecurity threats are challenging organizations in every industry, including the public sector. Over the past three years, DOE has been the target of multiple cyber-attacks. While our defenses have significantly evolved in response to these incidents, the cybersecurity threats continue to adapt as well. To that end, we have taken numerous measures to secure Departmental data, along with the personal information of our workforce. For example, we continue to strengthen the Joint Cybersecurity Coordination Center (JC3) to improve incident detection and response across multiple Federal agency partners. In addition, we have identified improvement areas in our cybersecurity training programs and established an executive-level Cyber Council to integrate cyber-related activities across the Department. As cybersecurity threats continue to become more frequent, persistent, and sophisticated in the years ahead, we will increase our vigilance by aggressively expanding our ability to prevent, detect, and respond to enterprise cybersecurity threats.

According to a GAO study, the number of cybersecurity incidents reported by Federal agencies increased by 782% from FY06 – FY12.

[1] *The DOE information ecosystem is defined as all people, processes, and technology that comprise the shared and unique services that will be supported by a joint security architecture and have a common set of enterprise information standards.*

Increasing Number of Federal IT Mandates and Cross-Agency Initiatives

In recent years, the Office of Management and Budget (OMB) and other Federal agencies have issued a stream of government-wide IT mandates and cross-agency initiatives aimed at creating a more transparent, efficient, and secure Federal government. In FY10, OMB unveiled a "25 Point Implementation Plan to Reform Federal Information Technology Management," which requires agencies to pursue efforts such as data center consolidation and a "cloud-first" policy for new IT deployments. Since then, a number of additional government-wide initiatives have reaffirmed and expanded the basic tenets of OMB's 25 Point Plan, including PortfolioStat, which guides agencies to reduce wasteful IT spending by conducting an evidence-based review of their IT portfolios. In FY12, DOE completed its initial PortfolioStat review, identifying more than $10 million per year in savings and cost avoidance. In addition to these mandates, openness and transparency have also emerged as critical reform efforts with the release of the FY09 Open Government Directive, FY12 Digital Government Strategy, and FY13 Open Data Policy. We have embraced these mandates by releasing high-value data to the public and developing applications designed for mobile computing devices and smartphones. As additional Federal IT reforms are introduced over the next four years, we will comply with existing and future government IT mandates and cross-agency initiatives.

From FY11 to FY13, the Office of Management and Budget issued more than 30 new mandates that impact DOE information and IT operations.

Maintaining a Skilled IT Workforce

As the Department's information ecosystem becomes increasingly complex, we will be challenged to supply the necessary talent to deliver tomorrow's technology. Specifically, due to the rapid pace of technology advancement, the Department faces the challenge of aligning new mission-driven IT staffing needs with employee skills, thereby leaving the Department vulnerable to skill mismatch and competency gaps. Nonetheless, in FY13 we made progress towards reducing skill gaps by implementing improvements to the IT Project Management Qualification process to ensure all Federal project managers for key IT investments were certified. In the future, working closely with the Office of the Chief Human Capital Officer, we will continue to support the Department's objective of developing a highly qualified, capable, and flexible Federal workforce. We recognize the need to identify existing and forecast future skill competency gaps, develop appropriate succession plans and knowledge management solutions to mitigate the risk of our retirement-eligible workforce, standardize enterprise-wide training, and instill forward-leaning competencies such as open data and information lifecycle management.

A subset of total Departmental IT training, DOE OCIO employees completed more than 2,000 hours of training in FY13 to continually improve their proficiency in mission-critical IT support functions.

Increasing Federal Budget Pressures

The current budgetary environment requires all Federal agencies, including the DOE, to execute their missions with a fiscally conservative mindset. Over the past five years, we have faced growing pressure to do more with less within the IT arena. In response to this trend, DOE has achieved significant savings through a number of IT efficiency initiatives including email consolidation, unified communications improvements, and commodity IT contract reductions. To achieve additional IT efficiencies while maintaining required service levels, we must minimize IT redundancies and complexity, decrease resource requirements to deliver commodity IT services, and embrace innovative, cost-effective strategies and technologies.

From FY10 to FY13, the Department generated significant cost savings by closing six Federal data centers.

Information Consumers and Stakeholders

From FY 2014–2018, we will undertake a number of strategic endeavors that will allow us to advance the Department's IT in an efficient and secure manner. To do so, we will be required to collaborate with a diverse group of internal partners and external stakeholders.

We have a large number of **information consumers** with varying functions and responsibilities, and consequentially, differing information and IT solution needs. Supported by recent open data government initiatives, the **public** is our largest information consumer group, using freely available Department data and information for individual consumption. Internally, we have three distinct consumer segments, each with drastically different needs: Office of the Under Secretary for Nuclear Security, Office of the Under Secretary for Science and Energy, and Office of the Under Secretary for Management and Performance. Across these mission areas are the **Departmental Elements**: 10 Program Offices, two independent DOE administrations, 15 Staff Offices, 17 national laboratories, four power marketing administrations, and eight Field Sites.

- **Program Offices** are based at DOE headquarters in Washington, DC and direct the policies and programs to carry out the Department's mission.
- **Independent DOE Administrations** include the Energy Information Administration (EIA) which is responsible for independently collecting statistical information about energy production and use, and the National Nuclear Security Administration (NNSA), a separately organized agency within DOE, which supports programs related to the Nation's nuclear weapons management, nuclear non-proliferation, and naval reactor programs.
- **Staff Offices** provide administrative and oversight support to Department programs and offices.
- **National Laboratories** perform cutting-edge research in science and technology to advance the Department's mission.
- **Power Marketing Administrations** are responsible for marketing and delivering hydroelectric power generated from Federal water projects. Each power marketing administration operates in a different geographical area of the country.
- **Field Sites** are offices outside headquarters that perform activities to support one or more Program Offices.

We also continually coordinate with a number of **government entities** that issue laws and mandates, policy decisions, and standards that influence the Department's information technology operations and strategic direction. For instance, the White House establishes government-wide priorities that shape our intra-agency information technology agenda, including digital government and open data initiatives. Moreover, we work with OMB to ensure that all Department information technology solutions are acquired and managed in a manner consistent with broader Administration goals. We partner with the Federal CIO Council to share best practices, learn about technology trends and priorities, and obtain useful Federal CIO resources. Additionally, we collaborate with the Government Accountability Office (GAO) to ensure the Department is meeting all Congressional information technology and cybersecurity governing policies. Further, we team with other Departments such as the Department of Homeland Security (DHS) and the Department of Commerce's National Institute for Standards and Technology (NIST) to advance Federal information technology standards and directives, including the Homeland Security Presidential Directive-12 (HSPD-12) governing identity management and NIST's Cybersecurity Framework. Finally, we partner with **innovators** from private industry and academia to gain expertise and discover, evaluate, and securely implement technologies in the DOE information ecosystem.

In the years ahead, we will strengthen our relationships with information consumers, government entities, and innovators.

"Advancing the DOE IRM mission requires close collaboration with Departmental information consumers, government entities, and innovators."

– Robert Brese, Chief Information Officer (CIO) for the Department of Energy

DOE IRM Mission and Vision

Information and IT are fundamental to advancing the Department's mission. IT automates business processes, improves the speed and flexibility of operations, and increases workforce productivity. In an era of shrinking budgets and mandated shifts towards a leaner government that uses private sector capabilities and shared services, we must effectively use current technologies and implement new and emerging technologies with a common Departmental mindset. By doing so, we can improve enterprise collaboration, business intelligence, and our cybersecurity posture. Accordingly, we have modified our mission and vision for Departmental information and IT.

The Office of the Chief Information Officer (OCIO) will lead this Departmental transformation, working in close coordination with all DEs. Moving forward, the OCIO will continue to provide some commodity IT services that it has provided since its inception such as desktop and worker productivity solutions, but this is no longer the sole focus of the OCIO's role. The OCIO will serve as the Department's advisor-broker for information technology. This model will benefit DOE by providing a dedicated body to focus on policy, governance, architecture, and standards, thereby influencing Departmental use and management of core infrastructure and commodity IT to meet mission outcomes and security requirements. To succeed in this role, the OCIO will strive to be the trusted advisor and enabler of the information ecosystem, encouraging DEs to seek the OCIO's support and insight on all technology solution initiatives.

This advisor-broker model allows the DOE CIO to strengthen the information ecosystem, benefiting all DEs. An improved DOE information ecosystem enables structured flexibility to meet mission support requirements while managing its complexity, ensuring effective interoperability and security, and delivering more efficient and reliable services. All of these outcomes support the evolving overarching mission of IT at DOE. As such, the DOE IRM mission statement establishes the Department's information and IT agenda for the next four years.

DOE IRM MISSION

Advance the Department's mission through policy, standards, and services, which meet mission requirements, balance risk and innovation, and set clear performance goals and expectations for the information ecosystem.

Complementing our mission statement is the DOE IRM vision statement, which describes the Department's aspirational, longer-term information and IT outcomes. To fully realize our mission it is essential that all Departmental information and IT initiatives are implemented with the focus of not only realizing cost-effectiveness, but also improving cybersecurity, quality of service, and Departmental collaboration.

DOE IRM VISION

Collaborate as an enterprise to deliver innovative information management and technology solutions that support the Department's mission.

Information and IT Core Capabilities

To realize our mission and vision we must develop and achieve proficiency in our information and IT core capabilities that underlie all strategies described in the DOE IRM Strategic Plan. These core capabilities include:

- **Governance:** We must establish and employ a streamlined, customer-driven Departmental governance capability to improve decision-making for IT investments. This includes rigorous Federal Capital Planning and Investment Control (CPIC), acquisition, investment review, and IT portfolio management processes.
- **Information and IT Management:** We must continue to modernize the way we manage our information and IT. Effective and efficient management of our information and IT operations is a key component of IT solution delivery. This competency relies on program management processes that align IT solutions with consumer expectations and mission requirements. In addition, the Department must maintain an ongoing commitment to innovation.
- **Enterprise Architecture, Policy, and Standards:** The Department's enterprise architecture describes the information landscape, components, and functions, thereby setting the boundaries for IT governance, policies, and standards. These policies and standards must be sufficiently detailed to provide predictability in IT deployments, yet agile enough to adapt to changing operating and customer needs.
- **Cybersecurity:** Protecting agency information and assets is paramount to successfully executing the Department's mission. We must proactively assess and detect cybersecurity risks and vulnerabilities, resolve threats when they do occur, and continually monitor the effectiveness of our cybersecurity solutions.
- **IT Workforce Management:** DOE must excel in IT workforce planning and management to support the Department's information technology needs. Key components of this competency include recruitment, development, management, and retention of DOE's IT employees.

Strategic Goals

The DOE IRM strategic goals build upon the three pillars established in the 2012 IT Modernization Strategy — *Transform, Protect, Advance* — and describe how we will achieve the DOE IRM mission and vision. For both classified and unclassified environments, *Transform, Protect, Advance* is an enduring commitment applied across our four strategic goals, which align information consumers' needs, efficient information solutions, a strengthened cybersecurity posture, and investments in our IT workforce and partners to further the Department's mission. Our IRM strategic goals are:

TRANSFORM
PROTECT
ADVANCE

STRATEGIC GOAL 1 "Supporting our information consumers"	Ensure delivery of high-quality information and IT solutions that meet consumers' needs and enable mission outcomes.
STRATEGIC GOAL 2 "Excelling as stewards of enterprise IT resources"	Safeguard our resources through the cost-effective management of information and IT solutions.
STRATEGIC GOAL 3 "Enhancing information security"	Protect the integrity of Departmental information by strengthening our cybersecurity posture.
STRATEGIC GOAL 4 "Investing in our workforce and partners"	Invest in our IT workforce and the partnerships required to advance the Department's mission.

In the following pages, we define the four goals in greater detail and describe how we will achieve them. Specifically, each goal is outcome-based and supported by several objectives, which are in turn supported by executable strategies.

GOAL 1

Ensure delivery of high-quality information and IT solutions that meet consumers' needs and enable mission outcomes

In today's digital age, information and IT solutions are integral to DOE's daily operations. Supporting the internal and external information consumers who depend on these solutions is a top priority for the Department. In the years ahead, we will broaden our understanding of our consumers' diverse needs and tailor delivery of information and IT solutions accordingly. To improve the usability, accessibility, and availability of information, we will modernize our information ecosystem while strengthening our data and information management policies. We will enhance our existing IT solutions and foster new ones to provide offerings that deliver maximum value to our information consumers. Our focus on delivering high-quality, consumer-oriented information and information technology solutions is paramount to the success of the Department's mission.

OBJECTIVE 1.1:

Improve delivery of enterprise information and IT solutions by understanding consumers' needs, preferences, and behaviors.

Information consumers have a wide range of needs and expectations related to the consumption and manipulation of information and IT. This broad consumer base – from the individual citizen to the diverse set of consumers within the various DEs – requires tailored solutions to meet its unique needs and preferences. Recognizing that a one-size-fits-all approach to IT is not sufficient, we have pioneered several initiatives to enhance the Department's ability to provide these solutions in a cost-effective manner. For example, in FY13, we established the Information Technology Point of Contact (ITPOC) initiative, a monthly working group of OCIO and customer representatives to exchange ideas on product and service delivery improvements. We also completed regular "house visits" to our internal information consumers and hosted the FY13 Customer Service Focus Workshop, where we discussed the current information consumer experience. Inputs from these activities, along with the annual Energy IT Services (EITS) Customer Satisfaction survey, are used to tailor solutions to meet consumers' needs.

The Department will become more proactive in providing products and services that meet and anticipate consumer segments' needs – distinguished by both Departmental Element alignment and job function – by offering solutions based on their usage behaviors. By more regularly interacting with our consumers, we will gain a detailed understanding of their preferences and expectations for value-added solutions. This feedback will enable the Department to enrich existing solutions, retire those that are outdated, and use pilot programs to introduce new offerings that will satisfy evolving consumer needs.

STRATEGIES:

- Identify information consumer segments to understand their unique role-specific needs and expectations for value-added functionality and service related preferences.
- Use consumers' feedback to improve, maintain, or retire solutions and their usage.
- Use a phased approach to test and validate expected improvements to the consumer experience.

OBJECTIVE 1.2:

Create new capacity through a network of DOE clouds that will achieve enhanced performance of information and IT solutions by integrating networks and services.

As the Department's mission becomes more heavily dependent on information and IT assets, there is an increasing demand for solutions that are easily deployed and consumed. This requires improving operational effectiveness, interoperability, and security, while reducing cost and space requirements. In FY11, we began an effort to reduce redundant infrastructure and services. For example, as of February 2014, we have closed six of our original 54 Federal data centers, and we plan to close four more by FY15. Also, in FY14, NNSA initiated the OneNNSA Network, which is an enterprise virtual Wide Area Network (WAN) that securely interconnects all NNSA Federal and Management and Operating (M&O) Sites and will facilitate enhanced collaboration across NNSA and DOE. Similarly, the Office of Science (SC) consolidated its IT infrastructure and implemented a WAN that interconnects all of SC's Federal sites, creating SC's private cloud.

Over the next four years, we will encourage the increased use of shared services with DEs and Federal agency partners, while co-developing appropriate service level agreements to ensure operational requirements are met. We will also continue to execute our Federal data center modernization and consolidation plan. Additionally, over time we will continue to progress the DOE information ecosystem towards an architectural model that uses Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Anything as a Service (XaaS) offerings. Through a combination of consolidation of commodity services to a minimum number of providers and federation of consolidated operating environments, we will strive to fully interconnect all DEs in order to maximize our employees' ability to collaborate seamlessly across the DOE information ecosystem in support of the Department's mission. These changes will increase user capacity, improve flexibility, reduce spending on redundant infrastructure and commodity services, and strengthen the security of our information.

STRATEGIES:

- Encourage the use of shared and XaaS services across Departmental Elements by increasing awareness of potential cost-reduction and service quality improvement benefits.
- Consolidate and shut down non-core data centers.
- Enable the secure delivery of underlying infrastructure (IaaS), platform (PaaS), and software (SaaS) services to be made available for use by all Federal organizations across the Department.
- Modernize current services, capitalizing on cloud technology to increase performance, strengthen security, and realize energy efficiencies.

OBJECTIVE 1.3:

Ensure the availability of and access to information that enables consumers to make timely, informed decisions by strengthening corporate data and information management approaches.

Access to timely, relevant data and information is essential to the Department's mission. In recent years, we have made progress to ensure information consumers have access to the right information at the right time. For example, in FY13, we improved the ability for consumers to query and analyze data through new tools on Energy.gov. These tools include: Application Programming Interfaces (APIs) for coders, federated search capabilities for government managers of open data, and specific search tools for students, regulators, and energy professionals. Similarly, in FY13, we initiated the Records Management Revitalization project which uses advanced technology and business processes to better manage our records inventory, address future capacity requirements, and enhance search and retrieval capabilities.

We will establish a Chief Data Officer position to develop and execute our Department-wide data strategy. We will offer enterprise data services to eliminate silos, improve the reliability of data, and reduce security risks. We will also provide public-facing data services that are open for all consumers to use. Moreover, we will use digital and traditional mediums to deliver and receive high-value data and information in an easily discoverable, retrievable, and recordable format that promotes transparency with appropriate consumers. We will continue to strengthen our electronic and paper records management capability. All of these efforts will be supplemented by providing training and communications to the DOE workforce on the importance of records management and sharing data and information in a secure manner.

STRATEGIES:

- Create a Chief Data Officer position to own and coordinate data and information management initiatives.
- Create specific data services that will be shared and accessible across the Department working in conjunction with role-based attribute access for consumers.
- Increase use of multiple channels to receive and deliver data and information in accordance with consumers' preferences and OMB guidance.
- Improve the records management program by establishing annual awareness training, developing an accurate, comprehensive records inventory, and formulating lifecycle management plans.
- Provide workforce training on the benefits, best practices, and requirements of securely sharing data and information.

OBJECTIVE 1.4:

Provide IT solutions by deploying innovative information technologies while enhancing existing technologies.

The Department's national laboratories are global leaders in the innovation of best-in-class information technology products and services. The national laboratories' value has only been limited by the lack of DEs' awareness of how they can benefit from the laboratories' innovations. We are committed to better recognizing and implementing technologies developed by the laboratories and other DEs to both improve existing and introduce new Department-wide IT solutions. In FY14, we established the foundation for the Technology Advisory Board (TAB), which will ultimately facilitate the transfer of information and innovative solutions with stakeholders from across the Department.

The Department will establish a formal, sustainable Federal technology transfer program to test and deploy innovative technologies. This will reduce the cost of new technologies necessary to meet Departmental Element requirements. We will provide solutions that enable consumers to access and use IT, while balancing security, efficiency, and value for the Department. Specifically, we will focus on IT such as Voice over Internet Protocol (VoIP) and Virtual Desktop Interface (VDI) thin client devices. Additionally, we will develop and implement a remote access environment that will enable the Department to more easily deploy and support a broader variety of mobile devices, such as corporate-owned, personally-enabled smartphones and bring your own device. Across all of these initiatives, we will continually identify and implement sustainable green IT to support the Department's energy reduction and environmental performance aspirations.

STRATEGIES:

- Develop processes to more quickly and efficiently deploy secure, innovative technologies.
- Implement services and tools that improve information consumers' ability to access and use IT.
- Provide and support a variety of mobile devices that permit greater work location flexibility.
- Identify and use green information technology to increase Departmental energy efficiency.

GOAL 2

Safeguard our resources through the cost-effective management of information and IT solutions

To meet the demands of our information consumers amidst a constrained budgetary environment, we must cost-effectively manage our IT resources. In the years ahead, we will improve our enterprise architecture and information policy standards to ensure all IT projects and programs optimize DOE resources and are operationally compliant. We will strengthen our enterprise IT governance processes to make corporate decision-making more efficient, transparent, and consistent. Finally, we will streamline and standardize our IT acquisition process to increase speed and reduce costs. Through each of these objectives, we will transform our IT management processes to operate as efficiently as possible.

OBJECTIVE 2.1:

Improve interoperability and compliance by enhancing Departmental enterprise architecture, policy, and standards.

The Department's federated nature creates an environment in which DEs have varying degrees of independence in establishing architecture, policy, and standards for information and IT. While this model enables the DEs to customize IT solutions that meet their specific needs, it makes information exchange, security vulnerability assessment, and IT infrastructure more complex. To enhance information exchange, in FY13, we implemented an enterprise architecture and portfolio management tool: Enterprise Architecture Roadmap Solution (EARS). Once it is fully deployed Department-wide, EARS will guide DOE DEs to optimize and secure their interconnected business architectures, strategies, and investments. Also, in FY14, we developed a bring-your-own-device directive, which describes DOE's policy that allows the Department's workforce to securely work from anywhere, at any time, and on the device of an individual's choice.

Building on our understanding of the current architecture, we will outline our vision for future-state enterprise architecture and associated improvements, resulting in a more efficient IT operation, greater visibility across the DOE information ecosystem, and increased flexibility to meet mission IT needs. To support migration to this future-state, we will establish Departmental policies that enhance interoperability, compliance, and quality. We will develop the governing standards to fulfill Departmental and relevant Federal policies. Finally, we will create and use a pricing model to standardize the way in which we communicate service fees to information consumers. This will allow consumers to fully understand costs and make informed decisions about which services are most useful.

STRATEGIES:

- Document the current and define the future-state Department Federal IT enterprise architecture to set boundaries for IT standardization.
- Develop Departmental information and IT policy to improve throughput and quality and fulfil Federal guidance and mandates.
- Define technical and data standards to achieve enterprise interoperability and meet Departmental and interagency policies.
- Develop a comprehensive pricing model, based on standard service level agreements, that includes a consistent, Department-wide chargeback model.

OBJECTIVE 2.2:

Improve Departmental decision-making by strengthening governance processes.

Governance fosters effective Departmental executive decision-making. We are committed to balancing Departmental Element independence and flexibility with the need for a centralized IT governance process. In FY13, the OCIO began to refine the Department's IT governance structure. In FY14, we will collaborate with the appropriate DOE mission stakeholders to build on these proposed revisions and ultimately develop a governance model that provides a forum for discussing and adjudicating corporate requirements, policies, and standards. The resulting IT governance board will inform budget and investment decisions, while overseeing the management of Departmental information and IT.

By engaging mission stakeholders throughout the establishment of the IT governance board, we will ensure that this governance model is institutionalized Department-wide to facilitate informed, cost-effective, and timely investment decisions. We will establish the OCIO as the Department's information and IT advisor to provide DEs with useful technical advice throughout the investment decision-making process. To increase visibility into the health of the Department's IT portfolio, we will make several IT financial and performance management improvements. Throughout all of our efforts, it is important that we continually improve our formal oversight of information and IT management and take measures to encourage voluntary compliance with established governance processes.

STRATEGIES:

- Establish an IT governance board and institutionalize its use to regularly conduct evidence-based investment reviews and adjudicate policy and standards decisions.
- Provide sound technical advice to enable Departmental Elements to make informed IT product and service decisions that align with Departmental policy and standards.
- Improve IT financial and performance management to make the health of the Department's IT portfolio more transparent and provide evidence to the governance board.
- Support Departmental oversight of and accountability for information and IT management by continually improving governance processes and publishing annual reports.

OBJECTIVE 2.3:

Increase the efficiency of Department IT investments by streamlining IT acquisition and improving project management processes.

In addition to improving governance, we must enhance our IT acquisition and corporate project management processes. We have already taken steps to streamline our acquisition processes, thereby increasing value to consumers and reducing costs. For instance, the Department consolidated contracts used to deliver commodity IT services, saving the Department nearly $1.5 million in FY13. In the same year, we developed tools such as the Corporate IT Project Execution Model (PEM) to improve Department-wide project management techniques.

Integration of the IT budget formulation, governance, acquisition, and project management processes is vital. This will facilitate a seamless flow of information throughout the investment lifecycle and simplify ongoing project operations. We will take steps to centralize applicable IT acquisition functions and seek strategic sourcing opportunities. We will also standardize enterprise IT project management and operations, including the use of agile methodologies, to more easily deliver successful IT projects on schedule and within budget. Finally, we will benefit from integrated project teams' expertise to accomplish enterprise-wide modernization priorities and address emerging needs.

STRATEGIES:

- Connect governance processes to appropriate IT acquisition and project management processes.
- Aggregate the acquisition function for IT investments to increase expertise and benefit from the collective buying power of the Department.
- Enhance corporate IT project management by providing common management tools and techniques and deploying integrated project teams for enterprise-wide projects.
- Capitalize on Department functional expertise to simplify operating procedures, achieve economies of scale, better serve information consumers, and refocus resources on core mission IT.

GOAL 3

Protect the integrity of Departmental information by strengthening our cybersecurity posture

Cybersecurity continues to be one of the most significant focus areas for DOE. Keeping the Department's mission-critical information, along with the personal information of our workforce, secure is a top priority for the Department. Accordingly, we are deeply engaged in a wide range of internal and interagency policy and operational activities. In the years ahead, we will undertake several initiatives to enhance our cybersecurity posture. We will strengthen situational awareness and incident response to address cybersecurity threats. We will establish federally-aligned Departmental cybersecurity standards, and introduce cutting-edge cyber technologies through our Cyber Sciences Laboratory and Cyber Innovation Center. In addition, we will improve cybersecurity training to bolster workforce awareness and accountability. For each of these initiatives, we will collaborate with our national laboratories, DEs, and interagency partners who are critical to defending the Department's information ecosystem.

OBJECTIVE 3.1:

Fulfill Federal security requirements by establishing standards and expectations for Departmental cybersecurity.

Strengthening the Department's cybersecurity posture is critical to the success of DOE's mission. Our path to improving Departmental cybersecurity begins with Federal security priorities: accountability, visibility through automation, and mature information security measurement. Since FY12, we have participated in the Cybersecurity Cross Agency Priority (CAP) Goal program, which encourages improved comprehensiveness and standardization of cybersecurity metrics reporting. While we have made noteworthy progress in implementing CAP Federal priority cybersecurity capabilities, including strong authentication, continuous diagnostic and mitigation, and Trusted Internet Connections (TIC), we acknowledge that our current CAP score indicates that we still have a significant opportunity to improve in each of these areas. Further, we comply with Federal Information Security Management Act (FISMA), Information Sharing and Safeguarding (IS&S), and other Federal cybersecurity requirements to provide secure and effective service to Department and public information consumers.

The Department will improve policies and controls while conducting continuous monitoring responsibilities and hardening the DOE infrastructure and network environment. We will continue to assess and embrace relevant standards developed by partners, reducing costs for the Department and speeding integration of new technologies. We will develop requirements and solutions that protect the privacy and confidentiality of the Department's information and resolve known vulnerabilities. This will provide greater transparency to data and information entering and exiting our network, the IT components that reside in our information ecosystem, and the users on our systems. Likewise, we will strengthen our accreditation standards to better safeguard our information and prevent insider threats. Across all of these efforts, we will expand our continuity of operations and disaster recovery capabilities.

STRATEGIES:

- Develop policies that direct the use of automated tools, strengthening of internal controls, and standardization of processes to reduce the cost and management complexity of cybersecurity functions.
- Implement cybersecurity measures that harden the Departmental infrastructure and network environment.
- Adopt standards and processes to accelerate the secure integration of innovative IT solutions.
- Design cybersecurity requirements and solutions that ensure Department information is appropriately protected.
- Execute the Department-wide approach to identity, credential, and access management to control accessibility of Department information, systems, and facilities.
- Ensure all mission-critical applications and infrastructure have sufficient continuity of operations and disaster recovery capabilities.

OBJECTIVE 3.2:

Prevent and promptly resolve cybersecurity threats by strengthening Departmental situational awareness and incident response.

Ad hoc security responses have limited value in today's rapidly evolving information ecosystem, since adversaries are continually adapting to defenses and creating new threats. To improve security, the Department has prioritized enterprise situational awareness to effectively gather actionable intelligence and direct cybersecurity resources. A key component of this effort is the Joint Cybersecurity Coordination Center (JC3), which provides a unified and standardized approach to cybersecurity data collection, incident response, and reporting across the Department, while allowing individual DEs to develop unique cybersecurity strategies that complement their mission objectives. JC3's ability to consolidate disparate cyber response functions and streamline information sharing provides the Department with tools to strengthen our overall security posture.

The Department will implement a proactive cyber risk management program to assess the risks associated with IT acquisitions and major enhancements. We will improve cybersecurity understanding and responsiveness through the use of distributed analytics and real-time collaboration. These efforts will be aided by the JC3, which once fully operationalized, will become a hub for information sharing, shared analytics, and collaborative incident response. JC3 will be supplemented by active defense capabilities and tools identified by our continuous diagnostics and mitigation (CDM) program. Finally, we will deploy our assets across the enterprise so that all Department sites benefit from enhanced cybersecurity services, including tools designed to harden the overall security of the bulk electric system.

STRATEGIES:

- Apply cybersecurity risk management assessments to ensure IT acquisitions meet legal and regulatory requirements prior to integration into the Department's information ecosystem.
- Enhance shared analytics and real-time information sharing and reporting to improve enterprise cybersecurity situational awareness.
- Improve coordination of Department-wide cybersecurity incident detection and response.
- Augment and support enhanced cybersecurity services at all Department sites.

OBJECTIVE 3.3:

Develop and transition cutting-edge technologies into the DOE security architecture by advancing the Cyber Sciences Laboratory and the Cyber Innovation Center.

The Department's ability to prevent, detect, and resolve cybersecurity threats is highly dependent on the use of cutting-edge cyber technologies. To accelerate national progress in cybersecurity technology and operations, we have established the Cyber Sciences Laboratory (CSL), a virtual cyber defense Research and Development (R&D) capability that combines researchers from DOE national laboratories, academia, and private industry. In FY13, the CSL made significant progress towards implementing a comprehensive Departmental cyber defense R&D program by establishing a formal governance process and publishing a research vision and roadmap. These achievements provide the foundation for future research and IT deployment efforts.

We will develop a DOE cybersecurity R&D investment portfolio that addresses future enterprise requirements, enhances broader Federal government capabilities, and strengthens the Department's support of the energy sector. Further, we will continue to use the CSL to accelerate research in areas such as scalable testing of system cyber dynamics, resilience and assurance, and big data and behavioral cyber analytics. To complement the CSL's research efforts, we will establish a Cyber Innovation Center – an integrated research hub – to collaborate with early to mid-stage innovators from the private sector and academia on forward-leaning cybersecurity technology. Internal coordination among the Departmental Elements, DOE Chief Technology Officer, CSL, and Cyber Innovation Center will be fundamental to our success. Finally, we will deploy the most successful cyber technology innovations throughout the Department, while making them available to our interagency government partners in accordance with applicable legal requirements.

STRATEGIES:

- Establish a Departmental cybersecurity research and development investment portfolio.
- Advance the Cyber Sciences Laboratory to improve cross-organization cybersecurity research and development efforts.
- Establish and mature a Cyber Innovation Center to strengthen joint cybersecurity innovation efforts.
- Evaluate and fund cybersecurity technology pilots with the potential for future Department-wide adoption.
- Transition applicable innovative cybersecurity technologies into the Department's information ecosystem.

OBJECTIVE 3.4:

Promote enterprise cybersecurity awareness and foster a stronger sense of accountability by improving cybersecurity training and communication.

Our workforce is an integral component of our cybersecurity defenses, as cybersecurity is everyone's responsibility. Universal cybersecurity awareness, behaviors, and skills improve the Department's ability to promptly identify, evaluate, and counteract potential threats. To prepare our workforce for modern security demands, we are enhancing our Departmental cybersecurity training and workforce development program, and partnering with the Department of Defense to reduce costs by sharing common training resources.

In the years ahead, we will provide the necessary communications and training to ensure all DOE Federal and contractor employees, regardless of job function, understand their role in safeguarding Department information from external and internal threats. We will seek opportunities to improve and provide Department-wide cybersecurity training along with role-specific training for our cybersecurity workforce. In addition, we will continue to use our knowledge base to assist our interagency partners and contribute to Federal and commercial efforts to advance cybersecurity innovation.

STRATEGIES:

- Provide relevant information to all DOE employees about cybersecurity risks, thereby encouraging greater individual accountability and awareness.
- Identify opportunities to improve the current training curriculum and deploy proactive Departmental cybersecurity training and human performance assessment programs.
- Develop a highly-capable cybersecurity workforce through specialized, role-based training and development.
- Use deep cybersecurity expertise to provide vulnerability and mitigation consultation to partner organizations.

GOAL 4

Invest in our IT workforce and the partnerships required to advance the Department's mission

The Department's IT operations are conducted by a dedicated, skilled, and diverse IT workforce. By focusing on workforce planning – recruiting, training, and retaining top talent – we can enable our workforce to better serve all information consumers. We will support the IT workforce by ensuring access to useful and secure technology tools, simplifying processes, and promoting an approach to information sharing that encourages collaboration with the best of our academic, industry, and internal Department partners. As we pursue each of these workforce development initiatives, our IT workforce will be better positioned to advance the Department's mission.

OBJECTIVE 4.1:

Support the Department's information technology needs by building a talented, diverse workforce.

The IT workforce – comprised of both IT and cybersecurity professionals – is critical to advancing the Department's mission. We have improved workforce planning to address the challenge of waning budgets, pending retirement of key IT personnel, and in-house expertise gaps. Due to the increasing number of eligible retirees, succession planning is underway using National Defense University Development Programs and detail assignments to ensure our workforce is better positioned to advance into leadership positions. Further, we have required that IT employees managing multi-million dollar projects obtain an IT Project Management Qualification, ensuring they have the necessary skills to manage to cost, schedule, and quality. To retain employees, we recognize outstanding performance with monetary rewards, special act honors, quality step increases, and other innovative awards.

As the Department's information and IT needs evolve, we will advance IT workforce planning efforts, helping to meet workforce capacity and capability gaps. We will identify the current IT workforce across all Departmental Elements, and where appropriate, realign personnel to reflect both DOE and DE-specific modernization efforts. To supplement our current workforce, we will use innovative ways to bring quality talent to the Department such as exchanges with private industry, fellowships with academics, and executive on-loan programs. We will partner with the Office of the Chief Human Capital Officer to improve the hiring and onboarding processes and increase alignment between employees' skills and vacant IT positions. We will continue to provide training and professional development opportunities to our IT workforce, while recognizing high-performing employees. Finally, we will remain committed to succession planning and investing in the future IT leaders of our organization. Through these efforts, we will become one of the best places for IT professionals to work in the Federal government.

STRATEGIES:

- Eliminate redundant work and realign personnel and respective responsibilities to support both Departmental and DE-specific modernization efforts.
- Improve the ability to attract highly skilled IT professionals and simplify the hiring process for IT personnel.
- Implement a Departmental IT training program to reduce skill gaps and retrain Federal employees in mission-critical technical and business competencies.
- Provide IT personnel with career development opportunities that retain talent, encourage diversity, promote enterprise-wide collaboration, and build future leaders.
- Foster a culture that embraces performance-based human capital management to yield a high-performing and accountable IT workforce.

OBJECTIVE 4.2:

Enable the IT workforce to execute its responsibilities by providing useful, secure technology and processes.

The productivity of our IT workforce depends on the technology and processes used to execute daily work. Therefore, many of our recent efforts have focused on these two areas. For instance, in FY11 we implemented the Corporate Information Management Center (CIMC), which is a mission system that supports internal IT business processes. The CIMC automated multiple processes, including the Contract Funding Process, which tracks all contract financial, budget, invoice, and other administrative data in a single location and eliminates the use of standalone spreadsheets. By streamlining the Contract Funding Process, the CIMC has created a "single point of truth" for contract funding information, eliminated wasteful activities, and reduced reliance on email, allowing for faster access to critical information and increased process transparency.

We will empower our workforce by providing value-added, dependable technologies and processes, prioritizing simplicity and relevance. As such, the Department will determine the IT workforce's current and anticipated future facility, technology, and service needs. Once these needs are identified, we will securely provide performance enhancing technologies and improve existing processes to increase efficiency and encourage greater collaboration across the IT workforce. Where possible, we will automate processes and deploy self-service tools to minimize burden on our workforce.

STRATEGIES:

- Assess the IT workforce's needs for facilities, tools, and services required to enhance business performance.
- Provide the IT workforce with suitable facilities, tools, and services that meet both classified and unclassified work needs.
- Establish automated processes and self-service tools that reduce manual work for the IT workforce.

OBJECTIVE 4.3:

Promote an enterprise approach to information sharing that will foster innovation by collaborating with government, industry, and academic partners.

The Department partners closely with government, industry, and academia innovators to discover and deploy new technologies and share best practices. For example, in FY13 the Department's Chief Technology Officer established a formal, sustainable Federal technology deployment program to bring innovative solutions such as cloud computing and mobility solutions into the Department's IT portfolio. The Department also hosts a series of Innovation and Technology Summits that showcase Federal innovation and transformation on topics such as risk management and data analytics. Further, in FY13, EIA developed a National Energy Mapping System and launched an interactive energy disruption map that combines real-time data from EIA surveys, the National Hurricane Center, the Department of Transportation, and other entities, thereby creating a national asset that allows all information consumers and DOE partners to better see and understand the potential impact of a storm.

Building on these recent successes, we will establish new relationships and advance existing partnerships to promote information sharing and collaborative innovation. We will continue to implement partner-established policies and standards, while continually engaging with innovators to learn of new technologies and business practices. The most promising considerations will be further assessed and, if plausible, we will insert them in an appropriately secure environment. As we collaborate with an ever increasing number of partners, we will continually capture and share IT expertise using formal knowledge management techniques to promote enterprise awareness.

STRATEGIES:

- Continue to develop strong partnerships that improve data and information sharing and yield collaborative, mutually beneficial results.
- Support the development and implementation of government-wide information and IT policies and standards in conjunction with partners.
- Continue to engage external partners to discover, evaluate, and insert innovative technologies and business practices into the DOE information ecosystem.
- Capture and disseminate IT expertise by developing formal internal and external knowledge management networks.

Performance Measures

The DOE IRM performance measures will provide a tangible target for performance as well as the means for tracking progress over time. We will establish and track the following enterprise measures, using a balanced scorecard, to provide Departmental leadership with a comprehensive view of the organization's performance.

Strategic Goal	Measure	Description
Strategic Goal 1: *"Supporting our information consumers"*	**Modernization Cost Savings Reinvested into DOE Mission**	Measure the amount of savings from modernization initiatives, such as implementation of shared services and reduction of redundant infrastructure, that are reinvested into the Department's mission.
	Information Consumer Satisfaction	Measure the percentage of information consumers satisfied with DOE enterprise information and IT solutions.
	Information Availability Index	Monitor the availability, timeliness, and accessibility of information resources, including the measurement of information with backup components and contingency plans.
Strategic Goal 2: *"Excelling as stewards of enterprise IT resources"*	**Departmental Governance Process Compliance Rate**	Track the percentage of IT initiatives that correctly follow Departmental governance processes.
	Acquisition Efficiency	Measure the efficiency of IT acquisitions in the form of cost avoidance through strategic sourcing and monitor the speed of acquisitions efforts for various types of contract vehicles.
	Cost to Operate	Measure the cost for each Departmental Element to serve its consumers and operate information and IT solutions.
Strategic Goal 3: *"Enhancing information security"*	**Cybersecurity Environment Purview**	Measure the percentage of the Department's environment and infrastructure that is monitored.
	Enterprise Cybersecurity Health Score	Track incident, vulnerability, patching, application, configuration, and financial cybersecurity metrics, in addition to compliance with cyber-security standards and percentage of the DOE workforce that has received cybersecurity training.
	Cybersecurity Capability Maturity	Measure the maturity of our enterprise cybersecurity capabilities across ten domains: risk, asset, access, threat, situation, sharing, response, dependencies, workforce, and program management.
Strategic Goal 4: *"Investing in our workforce and partners"*	**IT Workforce Development Score**	Measure employee development by using a weighted score of measures, including the percentage of employees with completed Individual Development Plans, hours of training completed per employee, and the percentage of certified IT project managers.
	IT Workforce Engagement Index	Measure the DOE workforce's overall satisfaction and engagement.
	External Technology Collaboration Score	Measure the number of new technologies that are evaluated and potentially deployed into the DOE information ecosystem as a result of external collaboration.

Looking to the Future

While the DOE IRM Strategic Plan identifies the strategic priorities necessary to achieve our mission, we have also developed an operational plan – which includes plans for the Department's future enterprise architecture – to define how these priorities will be executed over the next four years. This operational plan, the DOE Enterprise Roadmap, will be reviewed and updated annually to ensure we are making tactical progress against the DOE IRM Strategic Plan.

SUCCESS FACTORS:

To achieve the strategic goals outlined in our DOE IRM Strategic Plan and execute against the DOE Enterprise Roadmap, we must ensure we are continually embracing the following key success factors.

- **Uphold accountability:** While the OCIO will provide the Federally-mandated leadership and direction in the execution of the DOE IRM Strategic Plan, ownership of and accountability for individual strategies will be spread across the Departmental Elements.
- **Monitor execution:** Using the balanced scorecard, we will clearly articulate targets and provide ongoing oversight to ensure each strategy is met and progress is tracked over time.
- **Collaborate across the Department:** We will encourage a collaborate-first culture to promote the transparency and coordination of all IT initiatives across the Department.
- **Allocate resources strategically:** We will monitor the Department-wide impact of new IT initiatives and request and allocate resources strategically to ensure success.
- **Communicate continuously:** Our workforce and stakeholders deserve and expect clear, consistent communications regarding the expectations for and progress against the DOE IRM Strategic Plan.

CONCLUSION:

IT leadership across the Department will ensure alignment to the DOE IRM Strategic Plan within their organizations and will work collaboratively to support the technical, managerial, and organizational changes necessary to execute this strategy, and ultimately, advance the mission of the Department.

STRATEGIC GOAL 1

Supporting our information consumers

STRATEGIC GOAL 2

Excelling as stewards of enterprise IT resources

STRATEGIC GOAL 3

Enhancing information security

STRATEGIC GOAL 4

Investing in our workforce and partners

U.S. DEPARTMENT OF
ENERGY

Office of the Chief
Information Officer