OCIO

FY 2012 - FY 2017

Strategic Plan

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

Vision, Leadership and Commitment…

Enabling the Future through Technology and Information

VIEW ONLINE AT

energy.gov/cio

Innovation.

Transformation.

Sustainability.

Teamwork.

Partnerships.

Table of Contents

Message from Michael Locatis, Chief Information Officer

The Department of Energy (DOE) Office of the Chief Information Officer (OCIO) has forged valuable partnerships by bringing together internal information technology (IT) resources, our National Laboratories, and strategic networks—both within and outside of the Department—to promote agency-wide innovation and effective operations that provide tangible, positive, high-value outcomes for our nation. We have an aggressive agenda to accomplish and are operating with urgency to enable the Departmental mission. The IT strategy has been transformed to meet the Department's demanding need. The strategy is designed to:

- Leverage existing information technology and expertise to maximize mission accomplishment and reduce costs
- Identify and foster new and emerging information technology to maximize mission accomplishment and reduce costs
- Provide Departmental IT governance, policy, and oversight processes to ensure secure, efficient, and cost-effective use of IT resources
- Ensure acceptable risk-based cybersecurity through enhanced enterprise situational awareness, development of near real-time risk management, and combating advanced persistent threats

To further assist, we are actively executing the 25 Point Implementation Plan to Reform Federal IT Management as part of our efforts and a critical element to DOE mission success.

The OCIO is committed to supporting the sharing of best practices across the federal IT community. Improving federal IT management requires not only knowing what does not work, but identifying what does work—and implementing it. Leading the Department's IT reform initiatives is an exciting privilege, and we intend to bring about positive transformation to better achieve the Department's unique mission.

1.0 DOE Strategy Overview

1.1 Department of Energy Mission and Goals

The mission of the Department of Energy (DOE) is to ensure America's security and prosperity by addressing its energy, environmental, and nuclear challenges through transformative science and technology solutions.

Goal 1: Transform Our Energy Systems
Catalyze the timely, material, and efficient transformation of the nation's energy system and secure U.S. leadership in clean energy technologies.

Goal 2: The Science and Engineering Enterprise
Maintain a vibrant U.S. effort in science and engineering as a cornerstone of our economic prosperity with clear leadership in strategic areas.

Goal 3: Secure Our Nation
Enhance nuclear security through defense, nonproliferation, and environmental efforts.

Goal 4: Management and Operational Excellence
Establish an operational and adaptable framework that combines the best wisdom of all Department stakeholders to maximize mission success.

In FY 2011, the Department updated its Strategic Plan. The Department has further integrated the Strategic Plan's long-term and intermediate goals into its annual performance budget. This performance structure establishes a concrete link between the Strategic Plan's goals and the Department's annual budget, performance metrics, and performance reporting.

1.2 Organization of the Department

The mission of the Department is carried out by National Laboratories and technology centers, Power Marketing Administrations, Program Offices, Staff Offices, operations and field organizations, the Energy Information Administration, and the National Nuclear Security Administration. Supporting these entities are over 100,000 federal employees and support contractors.

DOE's organizational structure is decentralized and aligned with its multiple missions. Department senior management provides strategic plans, EA plans, and guidance to Program Offices to guide program planning, decision-making, and investing. Program Officials are responsible for acquiring and implementing approved programs and investments to achieve performance goals. In this way, the Department ensures that within the decentralized organizational structure, all decisions and activities continue to support the overall strategic goals of the organization.

2.0 OCIO Strategy Overview

2.1 Office of the Chief Information Officer Mission and Goals

The mission of the Office of the Chief Information Officer (OCIO) is to enable the Department of Energy's urgent missions in energy, science and nuclear security through the power of information and technology in a manner that balances risk with required outcomes in programs that span from open science to national security.

DOE promotes effective operations by encouraging performance-based management and facilitating the restructuring of mission- and business-related processes, where appropriate, before making significant IT investments to improve the performance and cost-effectiveness of the Department's information management activities. In addition, the OCIO's Office of Cybersecurity implements and maintains a comprehensive cybersecurity program that is effective across DOE's diverse missions and large array of interdependent networks and information systems.

Strategic Goal 1: Leverage Existing IT
Leverage existing information technology and expertise to maximize mission accomplishment and reduce costs.

Strategic Goal 2: Foster New and Emerging IT
Identify and foster new and emerging information technology to maximize mission accomplishment and reduce costs.

Strategic Goal 3: IT Governance, Policy, and Oversight Processes
Provide Departmental IT governance, policy, and oversight processes to ensure secure, efficient, and cost-effective use of IT resources.

Strategic Goal 4: Risk-Based Cybersecurity
Strengthen enterprise situational awareness to foster near-real-time risk management and combat the advanced persistent threat; forge interagency and sector partnerships to protect critical infrastructure, promote information sharing, and advance technologies for cyber defenses.

2.2 Vision

The Chief Information Officer's (CIO) vision is to be the recognized partner that brings technology and programs together to unleash the power of information in achieving the DOE mission.

2.3 Goal Alignment

In accordance with OMB Circular A-130, the OCIO strategic plan supports the Department's strategic goals and direction. The table on page 8 shows the alignment of the OCIO strategic goals to the Department's four strategic goals. The OCIO goals are either directly aligned or a significant enabler for each strategic goal. A direct alignment is based on a clear linkage between the contribution of OCIO goals to the accomplishment of a mission, and an indirect alignment (noted as crosscutting) reflects linkages where OCIO goals create the technological or information sharing environment within which a strategic mission or goal is accomplished.

Alignment of OCIO Strategic Goals to DOE's Strategic Goals

DOE Goals OCIO Goals	Transform Our Energy Systems	The Science and Engineering Enterprise	Secure Our Nation	Management and Operational Excellence
Leverage Existing IT	Direct / Crosscutting	Direct / Crosscutting	Direct / Crosscutting	Direct
Foster New and Emerging IT	Direct / Crosscutting	Direct / Crosscutting	Direct / Crosscutting	Direct
IT Governance, Policy, and Oversight Processes	Direct / Crosscutting	Direct / Crosscutting	Direct / Crosscutting	Direct
Risk-Based Cybersecurity	Direct	Direct	Direct	Direct

2.4 Target Opportunities

The OCIO uses strategic plans and other management tools to ensure that IT decisions, management responsibilities, and accountability are positioned to meet the Department's present and future needs.

Coordinated with strategic planning, the OCIO uses Departmental processes such as Enterprise Architecture (EA), IT Capital Planning and Investment Control (CPIC), and technology assessment programs to identify opportunities to leverage both existing and new technologies to support Department goals. These processes aim to reduce performance gaps in the overall IT portfolio by retiring obsolete systems, developing new solutions that provide improved performance, and supporting the development of reusable application components.

This OCIO Strategic Plan highlights key initiatives and the path forward. With successful implementation, the actions described in this plan will enable the Department to best select, align, and maximize its IT resources to fulfill DOE mission.

2.5 IT Investment Portfolio

Each year, the Department selects IT investments that meet mission needs, close performance gaps, align with EA plans, and align with external drivers such as OMB's 25 Point Implementation Plan to Reform Federal Information Technology Management. The table below shows the breakout of DOE's Budget Year (BY) 2012 IT portfolio based on DOE strategic goals.

DOE Total IT Portfolio BY 2012

	Total Portfolio Funding	
DOE Strategic Goal	**Dollars (in Millions)**	**Percentages**
Transform Our Energy Systems	138.51	7.4%
The Science and Engineering Enterprise	594.06	31.8%
Secure Our Nation	1,130.10	60.4%
Management and Operational Excellence	7.98	0.4%
Total	**1,870.64**	**100.0%**

As indicated above, 100 percent of DOE's BY 2012 portfolio directly supports the four DOE strategic goals. The IT portfolio is characterized by a wide array of initiatives ranging in size and sophistication, all of which are aimed at mission accomplishment, improved operational efficiency, and support of crosscutting Department priorities such as sustainability.

3.0 OCIO Strategic Goals

The OCIO has IT strategic goals and objectives that drive achievement in DOE mission and strategic goal support.

Strategic Goal 1:	**Leverage existing information technology and expertise to maximize mission accomplishment and reduce costs**
Objective 1:	Implement a secure DOE federal infrastructure by improving IT services into a best-in-class provider from both a technical and business perspective
Objective 2:	Develop a comprehensive business management and contracting strategy to reduce the complexity and improve the agility of internal and external support contracts [25 Point Implementation Plan for Federal IT Reform]
Objective 3:	Generate substantial savings within OCIO and across DOE through the implementation of a comprehensive enterprise IT consolidation and sustainability plan [DOE Strategic Sustainability Performance Plan; Executive Order 13514; 25 Point Implementation Plan for Federal IT Reform]
Objective 4:	Establish the human capital and organizational foundation to create a high-performing organization [25 Point Implementation Plan for Federal IT Reform]
Strategic Goal 2:	**Identify and foster new and emerging information technology to maximize mission accomplishment and reduce costs**
Objective 1:	Establish a formal, sustainable federal technology deployment program
Objective 2:	Identify and leverage innovative service delivery methods [Federal Cloud First Policy; 25 Point Implementation Plan for Federal IT Reform]
Objective 3:	Identify and foster use of green technology to support energy use reduction goals [DOE Strategic Sustainability Performance Plan; Executive Order 13514]
Strategic Goal 3:	**Provide Departmental IT governance, policy, and oversight processes to ensure secure, efficient, and cost-effective use of IT resources**
Objective 1:	Implement and institutionalize a reformed, integrated information technology management governance process that treats M&Os distinctively different than true federal entities
Objective 2:	Establish and implement robust Departmental policy on IT issues and appropriate IT oversight processes [Clinger-Cohen Act; DOE Order 200.1A; OMB Circulars A-11 & 130]
Objective 3:	Revitalize the records management program to raise general awareness and develop plans [Federal Records Act; Paperwork Reduction Act; DOE Orders 243.1 & 243.2; 36 CFR, Chapter XII, Subchapter B]
Objective 4:	Establish strong cooperative internal and external partnerships that lead to effective information sharing and a mutually supportive relationship to achieving the DOE mission and applicable federal goals
Strategic Goal 4:	**Strengthen enterprise situational awareness to foster near-real-time risk management and combat the advanced persistent threat; forge interagency and sector partnerships to protect critical infrastructure, promote information sharing, and advance technologies for cyber defenses**
Objective 1:	Implement a proactive cyber risk management program that ensures appropriate and cost-effective security to enable missions and meet legal, OMB, and regulatory requirements [Federal Information Security Management Act; DOE Order 205.1B]
Objective 2:	Implement a cyber incident management program that enhances security of federal and M&O networks and provides enterprise-wide coordination and response [Federal Information Security Management Act; DOE Order 205.1B]
Objective 3:	Implement an enterprise continuous monitoring strategy to cultivate actionable intelligence and rapidly inform management action [Federal Information Security Management Act; DOE Order 205.1B]
Objective 4:	Promote highly-capable cyber workforce through specialized, role-based training and development [National Initiative for Cybersecurity Education]

3.1 Strategic Goal 1:

Leverage existing information technology and expertise to maximize mission accomplishment and reduce costs

The OCIO has established comprehensive functions to address policy, people, and processes related to IT management. By working from a sound organizational foundation and focusing on continuous improvement to meet new challenges, the OCIO will leverage an array of existing resources including human capital, contractual, and organizational processes to ensure effective IT management and strong mission support throughout the Department. Descriptions of targeted outcomes and actions related to this goal are described below.

Objective 1: Implement a secure DOE federal infrastructure by improving IT services into a best-in-class provider from both a technical and business perspective

The OCIO Office for Energy IT Services (EITS) has the responsibility to provide shared and crosscutting IT infrastructure to the federal community including the DOE-wide network, servers for application and data hosting, secure internet access, e-mail services, federal desktops, and helpdesk support. The EITS team works to provide efficient, low cost services consistent with service level agreements in place with customers from across the Department. EITS is focused on becoming the DOE commodity services provider of choice.

ESSENTIAL ACTIONS:

- Develop and deploy a virtual desktop infrastructure capable of supporting all DOE federal desktops, improving the interconnectivity between federal and M&O information resources, and providing device-agnostic connectivity
- Develop a five-year enterprise technology roadmap that outlines a near- and long-term technology migration path for future EITS services

TARGETED OUTCOMES:

- A standardized, simplified federal IT infrastructure
- Reduced number of components required to operate
- Reduced number of infrastructure sites and facilities
- Strengthened cybersecurity
- Shared services
- Increased operability and efficiency

Objective 2: Develop a comprehensive business management and contracting strategy to reduce the complexity and improve the agility of internal and external support contracts

The OCIO's business management and contracting strategy will have two major elements: establishing an Operational Information Technology Services (OITS) contract by late FY (Fiscal Year) 2011 and continued optimization of the current Enterprise Wide Agreements (EWA) Program.

As part of an overall IT acquisition framework, the OCIO seeks to leverage the cost savings and management efficiencies that result from acquiring and managing commodity IT products and services as well as commercially available software on a government-wide basis. Contract administration efficiencies are achieved by reducing multiple contracts to one and improved pricing is obtained by leveraging the Department's total buying power.

The OITS contract will be established in FY 2011 to consolidate and optimize commodity IT services throughout the DOE complex. Emphasis will be placed on maximizing use of this contract to decrease the DOE's IT total cost of ownership. This contract will also be structured to minimize subcontracting.

The OCIO's EWA Program is a collection of optional-use strategic sourcing contracts for common-use software, hardware, and services used within IT organizations across the Department. The EWA Program is structured to allow use by the entire DOE complex, including DOE Program Offices, Staff Offices, Field Sites, National Laboratories, and Power Administrations, and supports and complies with the Energy-Wide Strategic Sourcing (EWSS) Program, Federal SmartBUY initiative, Clinger-Cohen Act, and other legislative and DOE policies.

ESSENTIAL ACTIONS:

- Drive increased use of both the OITS contract and the EWA Program through an aggressive stakeholder communications and management program
- Reduce administrative cost of administering contracts by documenting and automating processes
- Optimize the EWA program to create more cost effective options for our customers
- Award new IT support services contract for current IT

TARGETED OUTCOMES:

- Maximized buying power and reduced total cost of IT ownership by attaining optimal pricing through the aggregation of software requirements
- Streamlined acquisition process to increase IT contract administration efficiencies through consolidation opportunities of legacy IT contracts into single contract vehicles and enterprise license agreements

Objective 3: Generate substantial savings within OCIO and across DOE through the implementation of a comprehensive enterprise IT consolidation and sustainability plan

By consolidating IT infrastructure as directed in the Federal Data Center Consolidation Initiative (FDCCI) and through the continued implementation and evolution of the Department's Strategic Sustainability Performance Plan (SSPP) the Department will cut costs while reducing its contribution of federal greenhouse gases. The SSPP contains electronic stewardship goals that focus on consolidating and reducing data centers and implementing improvements in the energy use at data centers. The OCIO has Departmental leadership responsibility for these efforts and is pursuing activities to consolidate IT services.

ESSENTIAL ACTIONS:

- Lead a Department-wide effort to identify and consolidate commodity IT services
- Develop and implement a federal data center modernization and consolidation plan
- Reduce the number of federal data centers by six (6) by FY 2015

TARGETED OUTCOMES:

- Reduced number of data centers
- Reduced real estate footprint
- Reduced data center costs
- Realized energy savings
- Increased resource-utilization rates
- Reduced costs of commodity IT services

Objective 4: Establish the human capital and organizational foundation to create a high-performing organization

The OCIO recognizes the strategic management challenge required to hire and retain a highly-skilled IT workforce and is working to address the criticality of strengthening human capital as a driver for organizational effectiveness. The Office of Management and Budget (OMB) has identified a specific human-capital initiative that is directed toward aligning a professional workforce in support of a Department's mission, goals, and strategies. The OCIO has developed recruitment requirements to focus efforts on identifying qualified candidates who are able to easily adapt to changes brought about by new technologies and is currently identifying gaps in skills and abilities of the current workforce, developing hiring plans, creating training and professional development plans, and documenting new, efficient business processes.

In addition, initiatives have been implemented to focus on maximizing employee performance by instituting development programs and enrichment opportunities that motivate and inspire employees. The OCIO will continue to recruit and retain new talent for critical management and mission-critical positions in order to achieve key objectives. As part of its strategic planning, the OCIO has established roles and responsibilities, high-level process flows, and an organization structure to position itself to become a high-performing organization.

ESSENTIAL ACTIONS:

- Leverage past effectiveness/efficiency reviews and new organizational and skills assessments to identify, plan, and implement changes to roles, responsibilities, and reporting relationships
- Re-align existing personnel resources to more effectively match existing skills to requirements
- Rapidly hire top-quality personnel as gaps are identified, particularly senior staff positions
- Strengthen performance-based personnel management
- Implement a new performance-management system to better recognize and reward superior performance ensuring a high-performing and accountable workforce
- Implement a performance framework for accountability at the employee level
- Implement a comprehensive training program to close skill gaps and sustain technical competence

TARGETED OUTCOMES:

- Aligned workforce skills to DOE missions and priorities
- Increased professional development within the federal workforce

3.2 Strategic Goal 2:

Identify and foster new and emerging information technology to maximize mission accomplishment and reduce costs

This strategic goal identifies the areas of focus and the processes by which new and emerging technology is assessed and can become an enabler to achieving the DOE mission. The OCIO's role in this area is to support Programs across the Department to identify and foster the acquisition and use of emerging IT to leverage new capabilities and rethink how to manage, communicate, and interact with departmental information.

Objective 1: Establish a formal, sustainable federal technology deployment program

The OCIO provides expertise and leadership to partner organizations across the Department in the identification of new and emerging technology that is useful in supporting the mission. To support this function, a Chief Technology Officer has been placed and an OCIO Office of Corporate Projects has been stood up to coordinate partnership, outreach, and technology research efforts.

ESSENTIAL ACTIONS:

- Develop and implement a technology innovation process to ensure well-formed input and handoffs to IT activities across the Department
- Define a process for effectively managing projects within the OCIO
- Refine the DOE IT Strategic Roadmap process
- Expand the OCIO's technology outreach and leadership via a series of summits

TARGETED OUTCOMES:

- Reduced cost of mission accomplishments due to more productive tools and processes
- Improved knowledge sharing

Objective 2: Identify and leverage innovative service delivery methods

The OCIO continually makes an effort to provide necessary mission support at the lowest possible cost and in the most transparent manner. By leveraging innovative service delivery methods such as on-demand infrastructure via cloud computing, the Department gains flexibility in mission support at low predictable costs.

The Department's cloud computing initiative is following the Federal Government's cloud computing direction for pursuing cloud as the preferred choice in capital projects. This initiative also supports the Federal Risk and Authorization Management Program (FEDRAMP) certification of private sector cloud alternatives. This initiative is closely linked to other initiatives, including, sustainability and data center consolidation.

ESSENTIAL ACTIONS:

- Identify and evaluate service delivery methods for use at DOE
- Implement cloud computing service delivery
- Identify and provide best practices in cloud computing acquisition
- Develop a sourcing strategy for innovative and emerging technologies, such as cloud computing, virtualization, mobile computing, etc.

TARGETED OUTCOME:

- Reduced costs of IT commodity services due to increased use of cloud computing and other innovative service delivery methods

Objective 3: Identify and foster use of green technology to support energy use reduction goals

Consistent with the overarching strategy of changing the landscape of energy supply and demand, the Secretary has established energy consumption reduction targets for the agency. Historically, IT operations have always required significant energy inputs. However, new technologies and strategies are constantly being developed for energy efficient IT service and operations. The OCIO is committed to identifying and leveraging new technology and techniques to ensure that IT is a significant contributor to the reduction of energy consumption Department-wide. The OCIO is pursuing activities to implement sound IT energy management practices that will result in reduced air conditioning costs and substantial energy savings.

ESSENTIAL ACTIONS:

- Promote energy conservation and paper waste reduction by raising awareness of preferred alternatives such as shared printers and duplex printing and the use of workplace multi-function devices
- Reduce (metered) electricity consumption to reflect office and desktop power management
- Improve Department-wide power management of desktop computers, printers, etc.
- Identify improved data center and space planning through the Energy Savings contract and public-private partnerships

TARGETED OUTCOME:

- Reduced Department-wide energy consumption and intensity by FY 2015, no less than 30% on average across the entire Department, relative to the Department's energy use in FY 2003

3.3 Strategic Goal 3:

Provide Departmental IT governance, policy, and oversight processes to ensure secure, efficient, and cost-effective use of IT resources

The OCIO provides leadership and coordination for Departmental IT management through effective IT governance, provisioning of IT policy, and the implementation of IT oversight processes related to enterprise architecture, IT investment management, and other crosscutting IT functions. By partnering with DOE Programs in governance and oversight processes, the OCIO ensures that IT services and assets remain aligned with mission needs.

Objective 1: Implement and institutionalize a reformed, integrated information technology management governance process that treats M&Os distinctively different than true federal entities

The OCIO is actively redesigning IT governance around its strategic goals and objectives and doing away with the disparate IT governance mechanisms that are often uncoordinated and result in poor management. The OCIO is rethinking its current governance structure and will refocus and coordinate governance groups to ensure appropriate participation, ownership, and accountability.

ESSENTIAL ACTIONS:

- Review and address IT issues using the appropriate governance groups
- Integrate and align existing governance groups including the Information Management Governance Council, Information Technology Council, and associated working groups

TARGETED OUTCOME:

- Establishment of coordinated governance groups and processes with appropriate authorities, roles, and responsibilities

Objective 2: Establish and implement robust Departmental policy on IT issues and appropriate IT oversight processes

As a decentralized Department, individual Programs and sites across the DOE complex perform the acquisition and management of IT resources. The OCIO is responsible for establishing policy and standards and overseeing Departmental IT management to the appropriate degree necessary to ensure consistency, interoperability, and security.

Implementing IT oversight processes ensures that the Department's portfolio of IT investments fully address DOE's business needs and strategies. The OCIO has successfully implemented TechStat, a face-to-face, evidence-based accountability review of an IT investment resulting in concrete actions to evaluate IT investments and to address weaknesses and turn around troubled investments. TechStat is vital to the Department's ability to improve line-of-sight between teams and senior management, and facilitates closer management of IT project progress with the ability to identify and address performance issues before they become costly to fix.

ESSENTIAL ACTIONS:

- Review and update IT policy and guidance to address changes in requirements
- Identify and address requirements for new policy and guidance in a timely manner
- Identify Headquarter and Field investments to be included in the TechStat Reviews
- Conduct TechStat reviews regularly at the Headquarter and Program levels
- Map OCIO policy to internal and external requirements
- Address gaps to ensure that a sound framework for IT management is established

TARGETED OUTCOMES:

- Maintained, completed, and up-to-date policy and guidance on IT acquisition and management
- Established appropriate IT oversight processes
- Increased precision of ongoing measurement of IT investment health
- Improved accountability with focus on concrete actions to improve performance

Objective 3: Revitalize the records management program to raise general awareness and develop plans

The Department has a renewed and reinvigorated emphasis on comprehensive federal records management at DOE. In an era of rapidly changing technology, records are being created and stored in a wide variety of formats and media. Traditional processes of records management must be updated to address this changing environment.

The Secretary of Energy and the Department are dedicated to having a comprehensive records management program whereby the systematic control of the creation, maintenance, storage, and disposition of federal records are ensured through the establishment of, and adherence to, standardized policies, processes, and the training of federal staff and contractors. The OCIO provides Departmental leadership and coordination of this effort.

ESSENTIAL ACTIONS:

- Develop a Department Records Management Tactical Plan
- Develop a records inventory and disposition schedule lifecycle management plan
- Develop and deploy a Department Records Management Training curriculum
- Provide recommendations for document management systems and RMA systems currently available

TARGETED OUTCOMES:

- Ensured uniform compliance with records management laws and practices through Departmental records management governance
- Updated Records Management policy via an improved DOE Order 243.1(B) that addresses previous shortcomings with regards to records management and vital records governance, management, and training
- Developed comprehensive (required) records management training that ensures all DOE employees and contractors understand record management requirements
- Implement Records Management Applications (RMA) to ensure the control and management of all “permanent” and “non-permanent” records across the Department, including e-mail

Objective 4: Establish strong cooperative internal and external partnerships that lead to effective information sharing and a mutually supportive relationship to achieving the DOE mission and applicable federal goals

The OCIO exercises leadership within and outside the Department through partnerships in support of Agency and Federal-wide initiatives. Such mutually supportive partnerships foster trust and communication and lead to the identification of IT management best practices.

ESSENTIAL ACTIONS:

- Establish mutually supportive relationships with DOE Program Offices, functional managers, and M&O CIOs
- Establish mutually supportive relationships with other federal agencies

TARGETED OUTCOMES:

- OCIO is a recognized business partner of DOE Program Offices, functional managers, and M&O CIOs
- Improved management of federal and private sector partner initiatives such as cloud computing, IPv6, and the Federal Risk Authorization and Management Program (FedRAMP)

3.4 Strategic Goal 4:

Strengthen Enterprise Situational Awareness to Foster Near-Real-Time Risk Management and Combat the Advanced Persistent Threat;

Forge Interagency and Sector Partnerships to Protect Critical Infrastructure, Promote Information Sharing, and Advance Technologies for Cyber Defenses

The Department's strategic path forward for cybersecurity aligns with Administration priorities which include delivering sector-focused cybersecurity solutions to the Defense Industrial Base (DIB) and providing leadership in the execution of the Comprehensive National Cyber Security Initiative (CNCI).

We know that to achieve its missions, DOE must be forward-focused in defending its diverse infrastructure and broad range of information assets. In collaboration with our National Laboratories and inter-agency partners, we are leading the technological advances necessary to secure our economic future and defend Government and critical infrastructure from increasingly sophisticated cyber attacks.

Objective 1: Implement a proactive cyber risk management program that ensures appropriate and cost-effective security to enable missions and meet legal, OMB, and regulatory requirements

The OCIO is leading the development of the Department's Risk Management Approach (RMA) for the Department's Cyber Security Program (CSP). This approach institutionalizes mission-focused risk management and line management accountability for ensuring appropriate protection of DOE information and information systems. The RMA and the CSP represent an extensive collaborative effort that exemplifies the Department's Strategic Goal to "Establish an operational and adaptable framework that combines the best wisdom of all Department stakeholders to maximize mission success." The RMA implements the four components of risk management (framing, assessing, responding, and monitoring) at all DOE organization levels.

The OCIO partners with the Office of Intelligence and Counterintelligence (IN) and the Intelligence Community to share critical threat information with the Federal community across security domains and rapidly inform DOE program risk management decisions to protect agency assets. The OCIO will continue to expand these efforts, while leveraging advanced research and development capabilities to mitigate the full spectrum of threats.

The RMA defines governance and processes for:

- assessing threats, analyzing risks, and sharing risk information through the corporate risk executive;
- informing risk-based decisions that consider mission assurance and cost-effective risk mitigation strategies, providing the appropriate benefit from available cyber security resources first;
- conveying assurance and conducting oversight; and
- ensuring consistency with guidelines from the National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) cyber requirements, processes and protections.

The RMA will implement automated enterprise Governance, Risk and Compliance (eGRC) capabilities to improve data collection, aggregation and reporting. This effort will reduce costs, re-direct resources and management focus towards operations, and improve OCIO customer service.

ESSENTIAL ACTIONS:

- Identify and document existing RMA capabilities including Contractor Assurance Systems solutions that could be leveraged in the target Enterprise capability
- Finalize RMA management plan to program inputs from Senior DOE Management
- Conduct and document RMA maturity assessment including reporting metrics that demonstrate increased situational awareness and improved Risk Management decision support

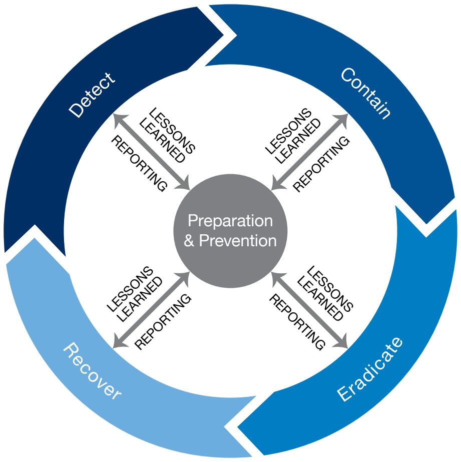
TARGETED OUTCOMES:

- Increased resource efficiency and automation
- Improved security posture and enterprise situational awareness
- Increased mission assurance; better informed risk management decisions

Objective 2: Implement a cyber incident management program that enhances security of federal and M&O networks and provides enterprise-wide coordination and response

The OCIO is partnering with the NNSA OCIO, the National Laboratories, and IN to develop the Department's next generation incident management capability. This initiative, known as the Joint Cyber Security Coordination Center (JC3) will integrate Departmental incident management capabilities into a coordinated response entity to provide front line cyber defense and Department-level situational awareness. JC3 will strengthen DOE's role as a leader in the national-level cybersecurity community through the timely sharing of DOE-derived cyber threat information with other agencies. JC3 will facilitate the aggregation, correlation, and deconfliction of inputs from Department-wide sensor networks and other data sources; provides computer forensic analysis; and conduct attack trending, tracking and mitigation of Advanced Persistent Threat. JC3 will coordinate incident management activities (Fxhibit 1) including prevention, detection, containment, and recovery for DOE Elements, and coordinate communications on behalf of the agency for cybersecurity events and emergency response with US-CERT and agency partners.

Figure 1: Incident Management Lifecycle



ESSENTIAL ACTIONS:

- Identify and document existing DOE Incident Management capabilities including M&O-sponsored solutions that could be leveraged in the JC3
- Develop JC3 governance model to include viable out-year funding model
- Finalize program management implementation plan; include plan for coordination of Management Executive Council-DOE Cyber Research and Development (R&D) Advance Technologies initiative
- Conduct and document program maturity assessment including reporting metrics that demonstrate increased situational awareness and improved decision support

TARGETED OUTCOMES:

- Documented enterprise baseline of requirements; map existing capabilities including National Laboratories' resources and expertise
- Improved DOE enterprise and Government-wide coordination for response to significant cyber events and Advanced Persistent Threat
- Improved enterprise-wide event management reporting
- Improved leveraging of R&D and advanced technologies to detect and prevent cyber attacks

Objective 3: Implement an enterprise continuous monitoring strategy to cultivate actionable intelligence and rapidly inform management action

OMB and Federal agencies have increasingly recognized the limited value of point-in-time security authorization for informing risk decisions and achieving effective risk management. The OCIO is leading agency efforts to develop Continuous Monitoring (CM) strategies that more effectively direct and utilize resources in protecting agency assets. This CM program will leverage the RMA and share OCIO eGRC capabilities to cultivate actionable intelligence and enhance decision support for the DOE and its stakeholders. In implementing the CM program, the OCIO will:

- Identify enterprise-level CM inputs necessary to build enterprise situational awareness and inform risk management decisions in near-real time (e.g. threat information, stakeholder communication flows, mission data, etc.)
- Define the process and periodicity for reviewing and updating policies, standards and procedures to maintain compliance with current statutory and regulatory drivers
- Describe how CM data will be aggregated, correlated, and analyzed to produce actionable intelligence and inform risk decisions including reporting.
- Develop a CM Implementation Plan that:
    - leverages existing resources first
    - deploys in phases to capture value quickly
    - describes knowledge chains and value points for organization
- Assess and measure program maturity; develop processes for continuous program improvement to include innovation through R&D and advanced technologies, optimization and lifecycle integration

ESSENTIAL ACTIONS:

- Identify and document governance, compliance requirements, models, and processes that impact and contribute to continuous monitoring
- Develop enterprise CM Strategy to include incorporation of advanced technologies and information sharing within DOE organizations and externally to the Federal community
- Conduct and document program maturity assessment including reporting metrics that demonstrate efficacy of CM Strategy

TARGETED OUTCOMES:

- Integrated multi-tier, continuous monitoring strategy that addresses governance, enterprise services, and system-level implementation
- Automated, common reporting process for DOE Headquarters Program and Site Offices
- Informed risk decisions using critical data flows that are identified and incorporated into CM plans

Objective 4: Promote highly-capable cyber workforce through specialized, role-based training and development

National workforce education and development initiatives such as the National Initiative for Cybersecurity Education (NICE) continue to underscore the critical importance of well-trained and capable cybersecurity workforce to execute the programs that support risk management and enable mission operations. The OCIO is leading the enhancement of the Department's cybersecurity training and workforce development program including partnering with Department of Defense to reduce costs by leveraging training resources. This effort includes a multiyear, multi-pronged approach toward developing and maintaining a training repository that maps training to critical cybersecurity roles and individuals with significant security responsibilities. The program is centrally managed through the OCIO, and will provide a full scope of advanced training resources and capabilities to assist all DOE Elements.

ESSENTIAL ACTIONS:

- Develop enterprise Cybersecurity Training Implementation Plan
- Establish communications plan to ensure critical roles are mapped to individuals, individual training plans are established, and completion rates are tracked
- Conduct and document program maturity assessment including reporting metrics that demonstrate efficacy of training program

TARGETED OUTCOMES:

- Increased workforce awareness and capability; improved mitigation of insider threat
- Improved security posture and workforce alignment with mission priorities
- Identification of key cyber security roles within each organization including documentation of individuals with significant security responsibility

Appendix A: Strategic Initiatives

Identity Credential & Access Management (ICAM)

This initiative establishes a framework for implementation of a variety of identity verification and access management capabilities. It addresses requirements related to HSPD-12 and enhances existing Public Key Infrastructure (PKI) capabilities. These key technologies enable the exchange of trusted identities across DOE and with other agency partners.

HSPD-12 - This investment brings the Department in compliance with Homeland Security Presidential Directive 12. The initiative provides an enterprise standards-based authentication and authorization infrastructure that offers secure, seamless business transactions and information exchange within DOE and across many disparate agencies and organizations.

The program will reduce existing logical and physical security vulnerabilities and mitigate risks to establish the prerequisite level of security for critical enterprise business functions. Both the technology solutions and ongoing support provided by the initiative will enable DOE to ensure that system users are who they claim to be (authentication), allow effective use of digital signatures (data integrity and accountability), and restrict access to appropriately authorized users (access control).

PKI - The mission of PKI Support Services is to provide electronic services related to authentication, confidentiality, privacy, data integrity, and non-repudiation through the use of digital identities, digital signatures, and two-factor authentication tokens. These services are available to all customers that have a valid business need to secure and transmit sensitive Department data, and/or the requirement to positively identify themselves to Department resources.

TARGETED OUTCOMES

- Provide a standardized DOE ID Card, compliant with HSPD -12 and capable of supporting physical and logical access requirements such as cryptographic storage of digital credentials, integrated standards-based building proximity support, and a printed format that complies with federal ID card requirements.
- Enhance a public key infrastructure solution that complies with federal standards, and supports DOE requirements for confidentiality, integrity and authenticity
- Implement an IIdentity, Credential, and Access Management solution that serves as the basis of a common security infrastructure that can support diverse systems
- Ensure DOE public/external facing servers and (web-enabled) services to use IPv6 by the end of FY 2012.

Sustainability and Federal Data Center Consolidation Initiative

This initiative addresses requirements under the Federal Data Center Consolidation Initiative (FDCCI), an OMB led initiative to consolidate and reduce the number of federal data centers. It also supports Departmental energy reduction and sustainability goals as documented in the DOE Strategic Sustainability Performance Plan. Data center reduction goals will be achieved through increased efficiencies such as the use of virtualization, consolidation of requirements, and implementation of increased use of cloud computing infrastructure as a service.

TARGETED OUTCOMES

- Reduce the number of DOE federal data centers by 6 by 2015

Performance Management Dashboards

The Performance Management Dashboards initiative works with Program Offices to develop business intelligence systems that inform senior DOE management about the effectiveness and efficiency of its program and financials. This initiative also includes the development of Science & Technology in America's Reinvestment Metrics (STAR METRICS) for measuring the effect of research on innovation, competitiveness, and science.

While this initiative is in the early stages, the goal is to use Program Office intelligence systems to leverage contractor assurance systems and improve the transparency of M&O contractor performance. This will provide DOE Senior Management visibility into contractor project performance much earlier enabling improved performance management.

TARGETED OUTCOMES

- Establish DOE intelligence systems that provide transparency and visibility into program and financial performance
- Provide Senior DOE Management timely performance information to support decision-making via the Performance Dashboards

Financial Assistance

The U.S. Department of Energy (DOE) provides a significant amount of financial assistance to support innovation and progress for America's energy, scientific, and national security needs, evaluating thousands of applications each year and awarding billions of dollars in financial assistance.

Due to the importance of DOE's investments and the impact of our research portfolio in supporting our national objectives and DOE's strategic plan, the DOE Deputy Secretary and Operations Management Council directed the OCIO to conduct an evaluation of financial assistance systems within DOE to determine the scope of the opportunity to modernize the underlying systems and services in support of financial assistance programs at the Department. Currently, DOE relies on a mix of systems and processes to administer financial assistance awards, ranging from in-house to outsourced products, and has no single system or tool to manage DOE's complete investment portfolio.

As a result, the OCIO has evaluated financial assistance technology solutions to identify an optimal approach, continuing our role of providing technology leadership, promoting innovation and effective operations across DOE. The recommendations promote a more integrated environment for coordinating executive insight into the financial assistance activities at the department and enable greater transparency.

In addition, the effort promotes DOE's federal leadership initiatives such as the STAR METRICS program, which provides a common empirical framework to identify outcomes of research investments and promotes the Department's commitment to science and innovation.

TARGETED OUTCOMES

- Identify an operational framework to manage financial assistance efforts and systems at DOE as a program.
- Enable DOE leadership for federal research and development activities through the STAR METRICS initiative.

Internet Protocol Version 6 (IPv6) Transition

The IPv6 Transition initiative ensures DOE infrastructure and application lifecycle management is aligned with the technical imperative and OMB direction to prepare federal agencies to use Internet Protocol Version 6 by 2014 (OMB Memorandum, 9/28/10). Agency deadlines include:

- Upgrade public / external facing servers and services by the end of FY 2012
- Upgrade internal client applications by the end of FY 2014

TARGETED OUTCOMES

- Successful and secure use of IPv6 by DOE infrastructure and applications in accordance with the OMB 2014 deadline

Technology Summits

The OCIO hosts a series of summits focused on advanced technology and innovation efforts across the Department and its partners, to highlight ways in which these activities help us succeed in our mission and contribute to success of the Nation's goals and grand challenges. This effort continues the OCIO's role of promoting innovation, showcasing technology leadership and identifying opportunities to modernize services and leverage the power of IT.

Through these types of forums, opportunities are communicated and discussed in an open, collaborative, environment and initiatives across DOE can be brought together to promote collaboration and information sharing. Individually, summits provide topical-based discussions, use cases and best practices that are linked to DOE and the OCIO's continual modernization and technology reuse initiatives and create greater awareness of the ways we engage in our mission.

Organizations participate from across the DOE enterprise including other federal agencies as well as public and private partners, and these discussions provide an opportunity to share stores and success, helping identify commonalities as well as an understanding of the unique circumstances encountered by individual missions and offices.

TARGETED OUTCOMES

- Enable the Department to develop a collaborative approach in developing insights to fuel IT transformation and mission alignment throughout DOE

Appendix B: List of Acronyms

ARB	Architecture Review Board
BRM	Business Reference Model
CAM	Corporate Asset Management
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CHRIS	Corporate Human Resource Information System
CNCI	Comprehensive National Cybersecurity Initiative
CNSS	Committee for National Security Systems
COTS	Commercial Off the Shelf
CPIC	Capital Planning and Investment Control
CRB	Corporate Review Budget
DIB	Defense Industrial Base
DOE	Department of Energy
EA	Enterprise Architecture
EATP	Enterprise Architecture Transition Plan
EAWG	Enterprise Architecture Working Group
EITS	Energy IT Services
ESNet	Energy Science Network
EVM	Earned Value Management
EWA	Enterprise Wide Agreement
EWSS	Energy-Wide Strategic Sourcing
FDCCI	Federal Data Center Consolidation Initiative
FEA	Federal Enterprise Architecture
FEDRAMP	Federal Risk and Authorization Management Program
FFP	Firm Fixed Price
FGDC	Federal Geographic Data Committee
FISMA	Federal Information Security Management Act
GLoB	Geospatial Line of Business
GPEA	Government Paperwork Elimination Act
GSA	General Services Administration
GSP	Geospatial Science Program
HSPD	Homeland Security Presidential Directive
IDEA	Innovative Department of Energy E-Government Applications
ICAM	Identity Credential & Access Management
ICPT	Integrated Contractor Purchasing Team
IM	Information Management
I-MANAGE	Integrated Management Navigation System
IOA&T	Infrastructure Office Automation and Telecommunications
IPT	Integrated Project Team
IPv6	Internet Protocol Version 6
IRM	Information Resources Management
IT	Information Technology
LOB	Line of Business
M&O	Management and Operating
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
O&M	Operations and Maintenance
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
RMA	Records Management Application
SPI	Spectrum Policy Initiative
SSP	Shared Service Provider
STAR	Science & Technology in America's Reinvestment

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

energy.gov/cio