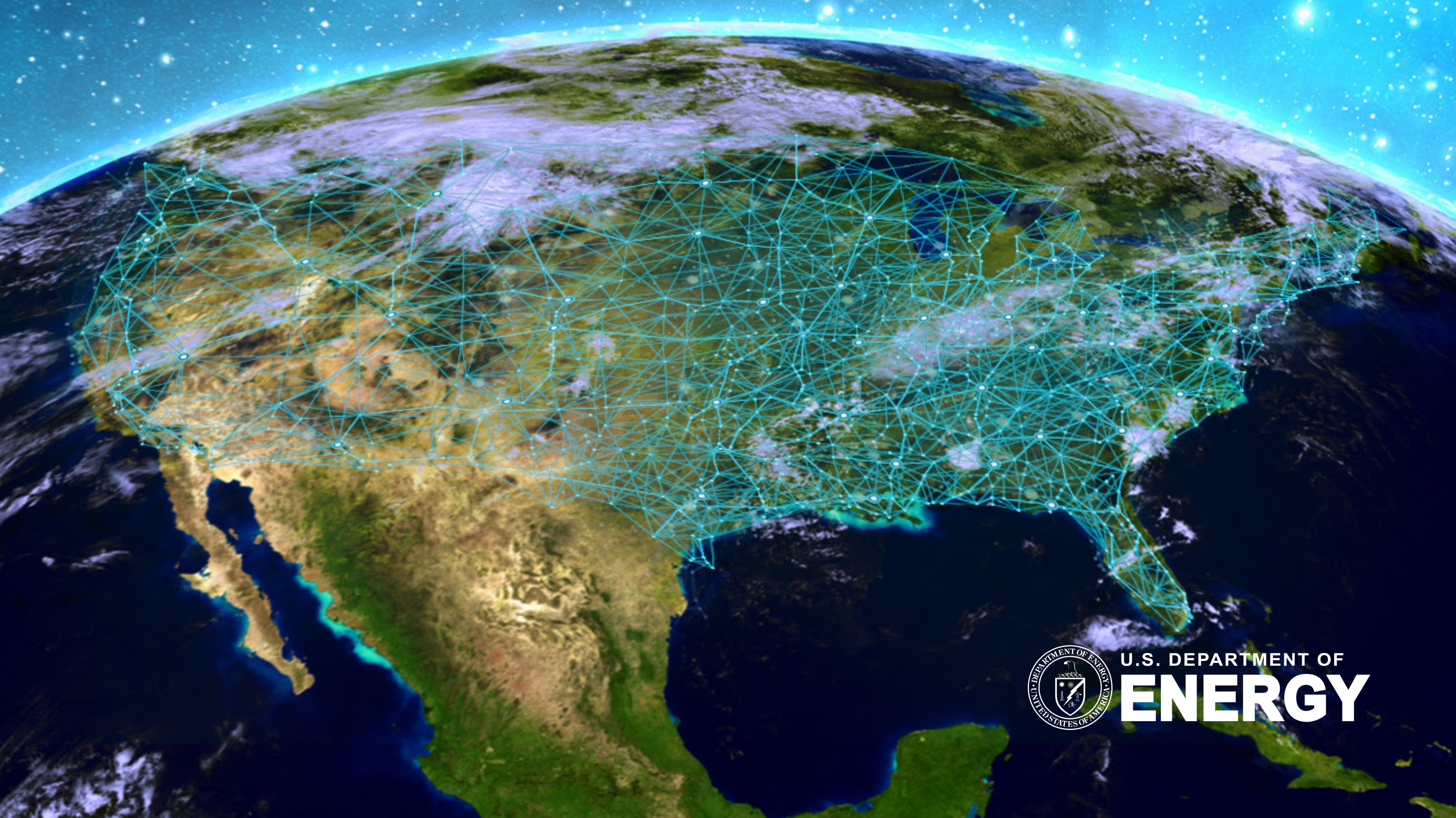
U.S. DEPARTMENT OF ENERGY

CYBER STRATEGY



U.S. DEPARTMENT OF ENERGY

TABLE OF CONTENTS

MESSAGE FROM THE DEPUTY SECRETARY

Dr. Elizabeth Sherwood-Randall
Deputy Secretary of Energy

> Across the Department of Energy we rely on digital technologies to gather, share, store, and use information that protects national security, enables groundbreaking research, and increases the efficiency of our operations.

Across the Department of Energy, our diverse missions are enabled by digital technologies. We rely on these technologies to gather, share, store, and use information. Because of our growing reliance on these technologies, we also increase our vulnerability to cyber threats that put our entire enterprise at risk.

As Chair of the DOE Cyber Council, I have guided the development and implementation of a new ***DOE Cyber Strategy***. This new Strategy sets forth DOE's enduring commitment to securing our cyber assets. Implementing this Strategy will enhance our ability to protect our critical infrastructure and to identify and report cyber incidents so that we can respond promptly and manage their consequences. It will also advance our nationwide efforts to work with other Federal agencies, as well as with state, tribal, local, territorial, private sector, and international partners.

Ultimately, it is the 115,000 women and men on our nationwide team, including our Federal, Management and Operating (M&O), and contractor workforce, who must do the work to keep us strong and safe. We must therefore partner across the Department, including DOE Headquarters, Program Offices, National Laboratories, Power Marketing Administrations, Plants, and Sites, to effectively anticipate and address cybersecurity vulnerabilities.

The priorities outlined in this important document are essential to realizing our cyber vision. I encourage every member of the team to read this Strategy and make a commitment to its full implementation. Together, we can transform and strengthen DOE's cyber enterprise in order to fulfill our vital missions on behalf of the American people.

Elizabeth Sherwood-Randall

MESSAGE FROM THE CHIEF INFORMATION OFFICER

Michael Johnson
Chief Information Officer (CIO)

The safe and secure stewardship of the Department's information assets is our top priority.

The Department's success in achieving its critically important national security, scientific, and energy mission rests on our ability to establish robust information sharing and safeguarding capabilities to ensure the security of information from increasingly sophisticated cyber threats.

To achieve the Department's cyber mission objectives, we must pursue information resources modernization and adopt innovative capabilities that enable advanced analytic techniques, information management and cybersecurity best practices, and enhanced partnerships with stakeholders.

The *DOE Cyber Strategy* is rooted in three fundamental principles:

- Information is a Departmental asset
- Effective information sharing and safeguarding requires a distributed, standards-based risk management approach
- Public trust is critical to mission success

Four strategic goals further articulate what we, as an enterprise, must do to advance DOE's cyber posture and ensure a strong combination of information sharing (mission enablement) and information safeguarding (mission assurance).

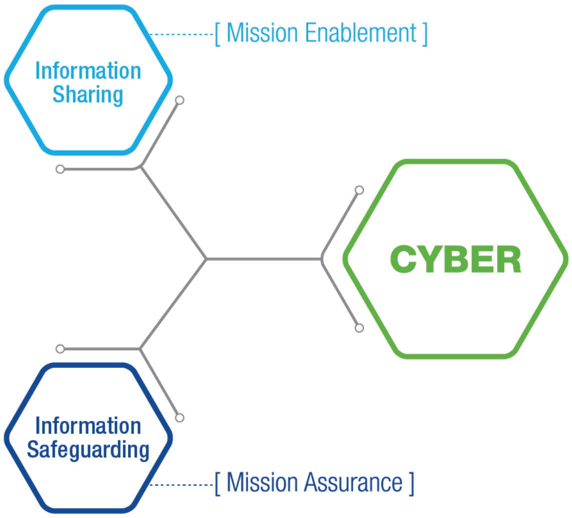
The ***DOE Cyber Strategy*** addresses the challenges associated with an increasingly complex cyber landscape. The approach to implementing this strategy requires a transparent, inclusive, and collaborative governance process across DOE Staff Offices, Program Offices, National Laboratories, Power Marketing Administrations, Plants, and Sites. Furthermore, we must successfully recruit, develop, and retain our most important resource, our people.

As CIO, I look forward to working with you to ensure this strategy's implementation, and durable success.

INTRODUCTION

Cyber poses a constant and dynamic challenge, with serious economic and national security implications for the Department of Energy (Department, DOE) and the United States. This is true for DOE Staff Offices, Program Offices, National Laboratories, Power Marketing Administrations, Plants, and Sites that comprise our "Energy Enterprise."

Today's rapidly evolving cyber landscape presents unprecedented opportunities and challenges. Achieving a safe, secure, and resilient cyber environment demands that we adopt innovative approaches and a full range of best practices. The Department's strategy must be agile and forward leaning. We must create an environment that prevents, deters, detects, and is resilient against cyberattacks, and minimizes the vulnerability of systems and networks.



Cyber is an enterprise-wide responsibility that demands an expanded view—beyond traditional cybersecurity—to encompass the broad scope of information sharing and information safeguarding.

Information sharing (mission enablement) ensures information is available and accessible to those who need it and are authorized to access and use it. Information safeguarding (mission assurance) ensures the protection of information essential to maintaining confidentiality, authenticity, privacy, and availability.

Managing the inherent tension between information sharing and information safeguarding is critical to the Department's mission and vision.

Building on past successes.

The *DOE Cyber Strategy* builds upon the Department's past successes and accounts for and addresses new and rapidly evolving cyber challenges. By employing threat-informed cyber intelligence, we will effectively safeguard and manage information as a Departmental and national asset.

Enterprise-wide collaboration is key.

The *DOE Cyber Strategy* articulates a compelling vision for the future, and a tangible plan for realizing it by leveraging diverse perspectives and experience from across the Energy Enterprise. By fostering a transparent and collaborative approach, we will establish a common understanding and a culture of accountability, tailored to the Department's unique structure and mission.

The Strategy identifies three crosscutting principles:

- Information is a Departmental asset
- Effective information sharing and safeguarding requires a distributed, standards-based risk management approach
- Public trust is critical to mission success

The Department will apply these principles across four strategic goals:

- Share enterprise information more effectively with authorized users
- Safeguard information against cyber threats
- Win the competition for cyber talent
- Mature and strengthen the Department's cyber posture

The success of the Strategy hinges on the Department's ability to collaborate and innovate. Building on this Strategy, the ***DOE Cyber Strategy Implementation Plan*** provides an essential roadmap with measurable objectives.

VISION

The Energy Enterprise will adopt a distributed, standards-based risk management approach to enable and ensure the Department's mission.

Information Sharing and Safeguarding

In alignment with the *National Strategy for Information Sharing and Safeguarding*, DOE's vision promotes secure and responsible information sharing that goes beyond a cybersecurity nexus to encompass all Departmental information that advances our mission. Our policies and practices build upon a vision that points to a future where the right information is provided to the right people at the right time, in a manner that rigorously protects national security, privacy, and civil liberties.

Mission success depends on enterprise-wide collaboration. By adopting a distributed, standards-based risk management approach, we will share information responsibly, ensuring the integrity and protection of the Department's cyber assets.

> “[We must] strike the proper balance between sharing information with those who need it to keep our country safe and safeguarding it from those who would do us harm. While these two priorities—sharing and safeguarding—are often seen as mutually exclusive, in reality they are mutually reinforcing... Our national security depends on sharing the right information with the right people at the right time. We will therefore keep working to maintain an environment in which information is shared in a manner that is responsible, seamless, and secure.
>
> President Barack Obama
> *National Strategy for Information Sharing and Safeguarding*

PRINCIPLES

Three foundational principles form the basis of our cyber vision.

Information is a Departmental asset.

The ability to share information continues to reach unprecedented levels. Recognizing that information technology is the true enabler of our mission, we view all information as a Departmental asset that must be discoverable and retrievable, consistent with necessary legal restrictions, and guided by government-wide policies, standards, and management frameworks.

Effective information sharing and safeguarding requires a distributed, standards-based risk management approach.

The Department will adopt enterprise risk management best practices, including a mature governance structure, integrated management coordination, and performance measurement. Our distributed, standards-based risk management approach allows Departmental elements to maintain decision-making authority based on widely accepted Federal and commercial standards, while also providing a flexible approach to enterprise-wide transparency and accountability.

Public trust is critical to mission success.

Transparency and consistency in the Department's privacy and civil liberties protection efforts is critical to maintaining the public trust. As a result, we continue to incorporate the technical, legal, and policy controls necessary to protect sensitive information in accordance with the law. By building protections into the development of information sharing and safeguarding efforts, we will ensure consistent application of privacy and civil liberties protections across the enterprise.

STRATEGIC GOALS AND OBJECTIVES

Strategic Goal 1: Share Enterprise Information More Effectively with Authorized Users

Effective information sharing unlocks data silos, spurs innovation, and improves the quality of services we can offer to the American people. DOE is committed to meeting the informational needs of stakeholders.

> Our national security relies on our ability to share the right information, with the right people, at the right time. As the world becomes an increasingly networked place, addressing the challenges to national security—foreign and domestic—requires sustained collaboration and responsible information sharing. The imperative to secure and protect the American public is a partnership shared at all levels including Federal, state, local, tribal, and territorial.
>
> *National Strategy for Information Sharing and Safeguarding*

Objective 1.1: Improve information sharing to support the mission.

The Department will provide stakeholders with discoverable, high-quality information, when and where they need it, with an emphasis on four key topics:

- **Information Availability:** Enable discovery and appropriate access to information
- **Architecture:** Design and implement modern, standards-based information technology and data architectures
- **Collaboration:** Facilitate a culture of communication and collaboration
- **Information Technology Enhancement:** Provide innovative solutions and enhance existing technologies

Objective 1.2: Adopt information management policies, guidance, and best practices.

We will transform the value of data by investing in cyber best practices and tools, standardizing existing sharing agreements, and providing the necessary frameworks (terms and conditions), such as:

- National Information Exchange Model
- Cybersecurity Information Exchange Framework
- Structured Threat Information Expression
- Trusted Automated Exchange Indicator Information
- Systems Engineering Body of Knowledge

Objective 1.3: Apply privacy and civil liberties protections to information sharing operations.

DOE will continue to strengthen privacy and civil liberties protections through policy, records management process controls, and data collection governance for storing, disseminating, and safeguarding information. Specifically, DOE will:

- Enhance access management processes consistent with laws, regulations, and national security interests
- Continue to apply legal and policy controls for collecting, processing, storing, using, sharing, and protecting information

Strategic Goal 2: Safeguard Enterprise Information against Cyber Threats

Protection of the Department's mission-critical information resources—both information and information technology—is our top priority. DOE continues to implement safeguarding solutions through continuous network monitoring, workforce communications and training, and advanced methods to identify, report, and mitigate insider threats and external intrusions. Information safeguarding demands continuous vigilance to detect and defend against adversaries.

> “[B]oth state and non-state actors are well financed [and] highly motivated in persistently attempting to breach both government and non-government systems… These attempts are not going away. They will continue to accelerate on two dimensions: first, the attacks will continue to become more sophisticated, and secondly, as we remediate and strengthen our own practices, our detection capabilities will improve. That means that we have to be as nimble, as aggressive, and as well resourced as those who are trying to break into our systems
>
> *Tony Scott, U.S. CIO*

Objective 2.1: Use threat-informed cyber intelligence to manage risk.

The Department is committed to implementing a distributed, standards-based risk management approach that uses threat-informed cyber intelligence to assess risk tolerance levels, categorize system readiness, and select associated controls. We will leverage established guidelines, including the Cybersecurity Capability Maturity Model, Cyber Security Evaluation Tool, and Electricity Subsector Cybersecurity Risk Management Process, to provide the common standards and reference points necessary to assess enterprise-wide capabilities and risks.

Objective 2.2: Develop and implement appropriate enterprise controls to reduce risk and become more resilient.

DOE will minimize security risks by increasing the use of strong authentication, controls on privileged access, audit assessments, and Identity, Credential, and Access Management processes by using a trusted framework and common identity infrastructure. Additionally, the Department will implement a standardized reporting mechanism and provide the workforce with communications and training programs on security policies and procedures, rules of behavior, and user awareness.

As a long-standing participant in the Cybersecurity Cross-Agency Priority (CAP) Goal Program, DOE will continue to integrate Federal priority cybersecurity capabilities, including continuous diagnostics and mitigation, and Trusted Internet Connections.

Objective 2.3: Develop tools and processes to accelerate notification of cybersecurity threats.

In response to increasingly complex cyber threats, we must develop the tools necessary to accelerate threat detection across the energy enterprise. Such tools will contribute to the advancement of the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership that provides critical infrastructure operators with the ability to share cyber threat data and analytics, and receive machine-to-machine mitigation measures in real-time.

The Department's ongoing collaboration with Information Sharing and Analysis Centers, such as the Electricity Information Sharing and Analysis Center, will continue to advance situational awareness, incident management, and communications capabilities.

Objective 2.4: Rapid analysis of, and response to, anomalies or suspected events.

To successfully deter and defend against cyber threats, the Department must be equipped to accurately detect hostile events. In collaboration with Federal and industry partners, DOE will develop cutting-edge cybersecurity solutions to strengthen and coordinate incident response capabilities, share resources, and provide situational awareness.

To combat advanced threats, the Department will implement a cybersecurity Incident Management Program (IMP), equipped with analytical forensics and response tactics. The IMP will include automated tools to streamline information technology security, improve incident management capabilities, and deliver training to frontline operators. This program will foster collaboration with industry partners, state, local, and tribal governments, as well as other Federal agencies—offering a comprehensive approach to incident management and response.

Objective 2.5: Develop and implement an incident triage, response, and recovery process to contain and eliminate cyber threats.

The Department will minimize the impact of cyber incidents by expanding continuity of operations, reducing recovery time, increasing resilience, and providing continued mission operations to our stakeholders.

Strategic Goal 3: Win the Competition for Cyber Talent

Cyber professionals are in high demand. It is imperative that we attract and retain an elite workforce in science, technology, engineering, and mathematics if the Energy Enterprise is to overcome rapidly evolving cyber challenges. To address this need, we will modernize the mechanisms by which the Department recruits, shapes, and retains a diverse and highly capable cyber workforce.

> “A high-performance organization needs a workforce with talent, multidisciplinary knowledge, and up-to-date skills in order to achieve its mission. To recruit such a workforce for cybersecurity, agencies should develop recruiting and hiring efforts that are tailored to address gaps in the number, skills, and competencies of their cybersecurity workforce. They should establish an active recruiting program with involvement from senior leaders and line managers and make use of strategies such as outreach to colleges, universities, and internships.
>
> *GAO, Cyber Security Human Capital*

Objective 3.1: Recruit a robust cyber workforce.

In an increasingly competitive environment, it is crucial that the Department prioritize the recruitment of leading talent by employing a range of incentives, including:

- Internships
- Cyber-based competitions
- Student loan repayment programs
- Cross-agency exchanges
- Executive loan programs

Establishing an enterprise-wide baseline will allow us to measure our recruitment efforts, identify mission needs, and anticipate future personnel requirements. These and other efforts will attract quality talent to DOE and nurture a sustainable, diverse workforce.

Objective 3.2: Develop cyber personnel.

We will cultivate a highly capable cyber workforce by providing advanced training programs and professional development opportunities, including cross-agency personnel exchanges, staff exchanges with private industry, and fellowships with leading academic institutions.

Objective 3.3: Retain cyber talent.

Our deeply committed cyber workforce is afforded the unique opportunity to make a large-scale impact to the Department’s critically important mission. We will continue to recognize our outstanding performers and encourage innovation. The Department will strengthen professional development processes, including succession planning, to facilitate employees’ transition into leadership roles.

Strategic Goal 4: Mature and Strengthen the Department's Cyber Posture

Our governance mechanisms must be modernized, streamlined, and strengthened to meet the Department's needs in a rapidly changing global environment. Additionally, we must evolve how the Department engages with federal, state, local, tribal, and territorial governments, the private sector, international partners, and academic institutions.

> “We will strengthen Department and national missions through crosscutting initiatives that leverage the science, technology, and engineering capabilities in program offices and the DOE national laboratories. The Department will continue to collaborate with other agencies, industry, the national laboratories, and academia to advance its missions and to foster technological innovation and technology transfer.
>
> Secretary Ernest Moniz
> *DOE Strategic Plan 2014-2018*

Objective 4.1: Enhance and inform decision-making using streamlined, inclusive, and transparent governance across the enterprise.

Recent Federal data breaches highlight the importance of effective governance. As we integrate the cyber expertise of Departmental elements, we will build a streamlined, inclusive, and transparent governance structure and eliminate organizational silos.

To mature and strengthen the Energy Enterprise, the DOE Cyber Council is dedicated to improving the Department's cyber posture, in conjunction with the Information Management Governance Board, which ensures situational awareness, strategic allocation of resources, and collaboration across the enterprise. This governance structure will:

- Ensure first-class membership of representatives from across the enterprise
- Implement enterprise-wide initiatives that bolster defense capabilities and coordinate responses to cyber threats
- Implement the Federal Information Technology Acquisition Reform Act to enhance DOE enterprise transparency
- Assess cyber posture to identify gaps and determine effective solutions for information resources management and cyber best practices across the enterprise

Objective 4.2: Advance the science of cyber to transform the Energy Enterprise.

To remain relevant in a rapidly evolving cyber environment, the Department will advance the science of cyber by investing in innovative technologies. As stewards of the public funds entrusted to us, it is our responsibility to establish clear goals and continually evaluate our progress.

Invest in cyber information sharing development:

- Mission-focused enterprise information architecture
- Network services to enable full enterprise visibility and coordination
- Secure enterprise information discovery capabilities
- Robust information access controls
- Enterprise unified data architecture and analytics platform, and associated shared services

Invest in cyber information safeguarding development:

- Information safeguarding architecture and solutions to include management and protection of high value assets
- Stewardship of key science, technology, and engineering capabilities
- Funding for the Cyber Sciences Laboratory
- Integrated cyber operations coordination, incident response, and intelligence through a single, integrated Joint Cybersecurity Coordination Center (JC3)
- Advanced analytics, forensic, and incident response capabilities
- Enterprise licensing of leading cyber defense capabilities

Objective 4.3: Foster interagency, public-private, and international partnerships to strengthen the Energy Enterprise.

The Department's future success relies in part on preserving and strengthening partnerships that foster innovative technologies and sharing of best practices. In accordance with the DOE Information Resources Management Strategic Plan, the Department will:

- Collaborate with international partners to capitalize on foreign investments and advancements in cyber
- Collaborate with private sector partners to commercialize new ideas in cybersecurity
- Develop and implement government-wide information and information technology policies and standards
- Engage external partners, such as the National Cybersecurity and Communications Integration Center (NCCIC), to identify and adopt innovative technologies and best practices
- Develop knowledge management networks to share cyber expertise

Objective 4.4: Measure enterprise cyber mission performance to inform decision-making, communicate value, and ensure accountability.

The DOE governance structure will apply consistent performance measurements that enable accountability, informed decision making, and continuous improvement. As the Department administers the DOE Cyber Strategy Implementation Plan, governance bodies will document and publish progress updates.

THE WAY FORWARD

As part of the Department's commitment to serve the nation as a leader in cyber, we will fulfill our mission to protect critical infrastructure and sensitive information, while safeguarding privacy and civil liberties.

Implementation Guidance

In alignment with the United States Chief Information Officer's 30-day Cyber Sprint Initiatives and the ***U.S. Cyber Strategy and Implementation Plan***, the ***DOE Cyber Strategy*** demonstrates the government's commitment to collaboratively protect Federal information resources and improve the resilience of Federal networks.

The ***DOE Cyber Strategy Implementation Plan*** will:

- Guide, measure, and track progress
- Prioritize initiatives and future needs
- Define desired outcomes
- Establish unity of effort, enhance transparency and accountability

Performance Management Guidance

In compliance with Federal law, DOE will implement a performance management program that assesses accomplishments, facilitates decision-making, holds leaders accountable, and demonstrates progress towards achievement of the Department's cyber vision.

APPENDIX - APPLICABLE MANDATES

The ***DOE Cyber Strategy*** incorporates more than 30 guiding documents, including Federal mandates and directives to strengthen information sharing and safeguarding. The core list of documents is as follows:

- 2012-2016 NNSA Implementation Plan
- 2015 Report on Configuration Management at the National Laboratories and Plants
- 25 Point Implementation Plan to Reform Federal IT Management
- Cybersecurity Risk Information Sharing Program
- Department of Energy Information Resources Management Strategic Plan FY2014-2018
- Department of Energy Laboratories: Leadership in Green IT
- Department of Energy National Laboratories and Plants: Leadership in Cloud Computing
- Department of Energy Office of Electricity Delivery and Energy Reliability, Energy Sector Cybersecurity Framework Implementation Guidance
- Department of Energy Office of the Chief Information Officer Strategic Focus Points
- Department of Energy Office of the Chief Information Officer Enterprise Roadmap
- Department of Energy Office of the Chief Information Officer FY2013 Human Capital Management Plan
- Department of Energy Office of the Chief Information Officer 120-Day IT Service Delivery Study
- Department of Energy Strategic Plan 2011
- Department of Energy Strategic Plan Update 2012
- Department of Energy Strategic Plan 2014-2018
- Department of Energy Information Technology Modernization Strategy
- Department of Homeland Security Information Sharing and Safeguarding Strategy
- Digital Government Strategy Report for the Department of Energy
- Digital Government: Building a 21st Century Platform to Better Serve the American People
- Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
- FY2012-2017 Department of Energy Office of the Chief Information Officer Strategic Plan
- Government Accountability Office: Report to Congressional Requesters, Federal Chief Information Officers: Reporting to OMB Can Be Improved by Further Streamlining and Better Focusing on Priorities
- H.R. 1232, Federal Information Technology Acquisition Reform Act

- M-16-03, Office of Management and Budget FY2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- M-16-04, Office of Management and Budget Cybersecurity Strategy and Implementation Plan for Federal Civilian Government
- Management and Oversight of Federal Information Technology (Office of Management and Budget Memorandum for Heads of Executive Departments and Agencies, 2015)
- National Information Exchange Model
- National Institute of Standards and Technology
- National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
- Office of the Director of National Intelligence Strategic Intent for Information Sharing
- Office of Management and Budget Circular A-130, Management of Federal Information Resources