U.S. DEPARTMENT OF
ENERGY | Office of Science

Cybersecurity Program Plan

v1.0

December 2020

Department of Energy Office of Science (SC)

Cybersecurity Program Plan

APPROVALS

Submitted by:

Gina M. Fisk Digitally signed by Gina M. Fisk Date: 2020.12.11 15:16:41 -05'00'

Gina Fisk, SC Chief Information Security Officer

12/11/20

Date

Concurrence:

Kelly N. Cummins Digitally signed by Kelly N. Cummins Date: 2020.12.11 15:11:07 -05'00'

Kelly Cummins, Associate Deputy Director for Field Operations

12/11/2020

Date

Approval:

Juston K. Fontaine Digitally signed by Juston K. Fontaine Date: 2020.12.11 15:25:52 -05'00'

Juston Fontaine, Deputy Director for Field Operations

12/11/2020

Date

VERSION CHANGE CONTROL TABLE

Version	Creation Date	Description	Approval Date
1.0	May 1, 2020	Original CSPP for SC	December 11, 2020

ACRONYMS

A&A	Assessment & Authorization
AAL	Authenticator Assurance Level
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authority to Operate
BOD	Binding Operational Directive
BDP	Big Data Platform
CAS	Contractor Assurance System
CDM	Continuous Diagnostics and Mitigation
CFM	Cyber Federated Model
CI	Counterintelligence
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Contracting Officer
COR	Contracting Officer's Representative
CPO	Chief Privacy Officer
CPP	Cooperative Protection Program
CRD	Contractor Requirements Documents
CSF	Cybersecurity Framework
CSM	Configuration System Management
CSP	Cloud Service Provider
CSPP	Cybersecurity Program Plan
CUI	Controlled Unclassified Information
DBS	Design and Build-in Security
DCS	Distributed Control Systems
DDFO	Deputy Director for Field Operations
DE	Departmental Element
DID	Defense In Depth
DISC	Data Discovery/Classification
DLP	Data Loss Prevention
DOE	Department of Energy
DOE-SC	Department of Energy Office of Science
EA	Enterprise Assessments
ECC	Electronic Country Clearance
ECGS	Enterprise Cyber Governance System
ECI	Export Controlled Information
ECN	Emergency Communications Network
ED	Emergency Directive
ESnet	Energy Sciences Network
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standards

ACRONYMS (cont.)

FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GIS	Geographical Information System
GSS	General Support System
HVA	High Value Assets
HWAM	Hardware Asset Management
IAL	Identity Assurance Level
IARC	Information Assurance Response Center
ICAM	Identity, Credential, and Access Management
ICS	Industrial Control Systems
iJC3	Integrated Joint Cybersecurity Command Center
IMGB	Information Management Governance Board
IN	Office of Intelligence and Counterintelligence
IOSC	Incident of Security Concern
IOT	Internet of Things
IRM	Information Rights Management
ISSM	Information System Security Manager
ISSO	Information System Security Officer
M&O	Management & Operating
MFA	Multi-Factor Authentication
MIA	Mission Impact Assessment
MIT	Data Breach/Spillage Mitigation
MNGEVT	Manage Events
NIST	National Institute of Standards and Technology
NLCIO	National Laboratories Chief Information Officers
NSS	National Security System
OCIO	Office of the Chief Information Officer
ODFSA	Officially Designated Federal Security Authority
OIG	Office of Inspector General
OMI	Operate, Monitor, and Improve
OT	Operational Technology
OUO	Official Use Only
PAO	Privacy Affairs Office
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PLC	Programmable Logic Controllers
POA&M	Plan of Actions and Milestones
PPOC	Privacy Point of Contact

ACRONYMS (cont.)

PRIV	Privilege Management
PROT	Data Protection
RMF	Risk Management Framework
S2	Deputy Secretary of Energy
SAO	Senior Agency Official
SAOP	Senior Agency Official for Privacy
SC	Office of Science
SCADA	Supervisory Control and Data Acquisition
SCIRT	Office of Science Incident Response Team
SCL	Sensitive Country List
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SME	Subject Matter Expert
SO	System Owner
SOP	Standard Operating Procedures
SOR	System of Records
SSP	System Security Plans
SWAM	Software Asset Management
TRUST	Trust Management
TSC	Technical Strategy Cell
UCNI	Unclassified Controlled Nuclear Information
U-NNPI	Unclassified Naval Nuclear Propulsion Information
VDI	Virtual Desktop Interface
VPN	Virtual Private Network
VUL	Vulnerability Management

Table of Contents

1 INTRODUCTION

1.1 PURPOSE

This Cybersecurity Program Plan (CSPP) implements DOE Order 205.1C for the Office of Science (SC) and all elements under its cognizance. It establishes a cybersecurity program that enables the mission of the Office of Science by ensuring a secure platform for scientific research and safeguards the ability to perform that scientific research. This CSPP also integrates risk-based cybersecurity into management and work practices across SC to ensure that scientific missions are accomplished while protecting all information on associated information systems.

1.2 CANCELLATIONS

This CSPP supersedes and cancels the Office of Science Program Cybersecurity Plan (SC PCSP) issued November 2016.

1.3 SCOPE AND APPLICABILITY

This CSPP applies to all SC offices and sites that collect, create, process, transmit, store, and/or disseminate information by or on behalf of the Office of Science. For the purposes of this document, SC headquarters and associated site offices are referred to as SC Federal sites, and M&O contractors are hereafter referred to as SC Laboratories.

The requirements in this document apply to unclassified systems that meet any of the following five conditions, with specific exclusions listed below.

1. The system was purchased by or on behalf of the federal government with federal funds, either directly or indirectly.
2. The system collects, creates, processes, transmits, stores, and/or disseminates information on behalf of the federal government.
3. The system is connected to SC infrastructure.
4. The system is at an M&O site and, upon a contract transition, would automatically transfer to the new contractor.
5. The system meets any of the previous four conditions and is a virtual instantiation in the cloud.

Specific exclusions include:

1. Systems purchased with federal dollars that are donated or loaned to educational institutions.

2. Systems purchased with federal dollars that are used exclusively for Cooperative Research and Development Agreements) CRADAs.

3. Classified systems with an Authority to Operate (ATO) from another government entity or DOE program.

4. Systems operated by a contractor solely for processing contractor-owned records as defined in *DEAR 970.5204-3, Access to and Ownership of Records (July 2005) – As modified by Policy Flash 2015-23* (May 2015).

5. Personal or experimental equipment belonging to collaborators that is connected to a guest network, defined as a network that is intended to be used for transient users to provide outbound internet access only and that is segmented or separated from the information and operations of mission, business, and production systems, and, requires that access to any internal resources be granted separately and strongly authenticated as approved by the risk-accepting official.

6. Specialized scientific equipment critical to performing the SC mission such as high-performance computers or high-performance networks that are unable to be secured, or whose scientific function does not behave properly in a cybersecurity-constrained environment. It is acknowledged that such scientific equipment must have a Mission Impact Assessment (Section 4.4) and approved Compensatory Controls (Section 4.5) for protection at an acceptable level as decided upon by the risk-accepting official.

1.4 GUIDING PRINCIPLES

The Office of Science's cybersecurity program is guided by the following principles:

1. Cybersecurity enables our scientific mission.

The Office of Science recognizes that cybersecurity is a mission-enabling function that provides a secure platform for innovation, collaboration, and agility and safeguards the ability to execute the mission. Efforts to mitigate cybersecurity risks must also support the scientific mission of SC.

2. **SC will effectively manage risk by taking a comprehensive, mission-informed, holistic approach to risk prioritization.**

   By prioritizing risk management, risk decisions and mitigation investments are focused on enabling operations while balancing risk, resources constraints, and the need for innovation.

3. **SC has a unique and diverse environment that requires unique and diverse security solutions.**

   The Office of Science has a diverse, "high-risk, high-reward" scientific mission, which includes state of the art supercomputers, one-of-a-kind accelerators, and a high-performance research network built to enable large-scale information collection and analysis with global partners. As such, SC will utilize novel solutions as needed to protect the mission.

4. **SC will utilize the successful M&O contractor model.**

   SC will manage the diverse environment and mission by placing responsibility on each SC Laboratory to develop methods of assessing, evaluating, mitigating, and monitoring risk.

5. **SC will continuously strengthen its cybersecurity posture.**

   The Office of Science will continually raise the bar each year to strengthen its collective security posture.

6. **SC will share expertise across the SC enterprise to make mission-informed cybersecurity decisions.**

   SC recognizes that our strength is in our people, whether they are federal employees or contractors, and that protecting our diverse scientific mission requires an open, collaborative approach across all SC Federal sites and SC Laboratories.

7. **SC will be a good steward of taxpayer dollars.**

   Efforts to increase our security posture must be continuously evaluated and reprioritized to ensure the best investments are made with taxpayer dollars.

1.5 CYBERSECURITY THREAT STATEMENT

SC Federal sites and SC Laboratories must protect SC systems from entities that seek to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threats to SC systems can come from a myriad of sources, including but not limited to hostile governments, criminal groups, foreign intelligence services, terrorist groups, disgruntled employees, and malicious intruders.

Threats to SC systems can come in multiple forms, including but not limited to botnets, spam, phishing, spyware, malware, denial-of-service attacks, insider knowledge or access, SQL injection, AI powered cyberattacks, electronic invoice fraud, ransomware, and zero-day exploits.

Though other threats exist, including natural disasters, environmental, mechanical failure, and inadvertent actions of an authorized user, the SC CSPP focuses on protecting SC systems from the deliberate threats mentioned above by using the NIST Cybersecurity Framework (CSF) and the NIST Risk Management Framework (RMF).

1.6 ANNUAL REVIEW

The SC CSPP must be reviewed and updated at least annually through a collaborative process.

1.7 INCORPORATING NEW REQUIREMENTS

DOE requirements are developed and promulgated through established processes outlined in DOE O 251.1D, Departmental Directives Program. In accordance with DOE O 205.1C, the DOE OCIO will develop non-binding amplification guidance through the DOE Directive Review Process, to provide a standardization baseline for key cybersecurity processes required by the DOE Cybersecurity Program. Amplification guidance will be aligned with FISMA, RMF, and CSF.

New or revised OCIO memoranda, DHS BODs, OMB directives, guidance, standards, policies, or requests will be assessed for Office of Science applicability and urgency. If the request is applicable, SC Site Authorizing Officials (AO), in coordination with the SC Chief Information Security Officer (CISO), will determine whether the request should be implemented as a new requirement in alignment with *DEAR 970.5204-2 (b)* for each SC Laboratory, implemented as a new requirement for the SC Laboratories with SC-specific tailoring, or if the request is consistent with existing contract requirements.

If the request is applicable to SC, the Site AO will develop a local risk decision and Mission Impact Assessment (Section 4.4) to include resource requirements for implementation of the OCIO request. The local SC risk decisions and Mission Impact Assessment (Section 4.4) and Compensatory Controls (Section 4.5) will be used to develop the Science implementation plan for the request once funding resources are identified.

In special circumstances of national security concern, the SC Enterprise AO may require specific security controls.

1.8 PUBLISHED LIST OF CYBERSECURITY CONTACTS

SC Laboratories and SC Federal sites must submit a current list of cybersecurity contacts to the SC Office of Cybersecurity (cyber@science.doe.gov) through the regular data call process, and update as necessary due to staff changes.

1.9 SC FEDERAL EXECUTIVE CYBERSECURITY ROLES AND RESPONSIBILITIES

The following section lists the cybersecurity responsibilities of key SC federal executives as outlined in DOE O 205.1C.

1.9.1 Director of the Office of Science

The Director of the Office of Science has the overall responsibility and accountability for the strategic direction of the cybersecurity program in SC, ensuring that it is mission-focused, cost-effective, and risk-driven. The Director establishes the overall risk tolerance of SC.

1.9.2 SC Deputy Director for Field Operations

The Deputy Director for Field Operations (DDFO) provides strategic direction and operational guidance for cybersecurity, enterprise information resource management, records management, privacy, data collection, paperwork reduction, spectrum, capital planning and investment control, cyber SCRM, FITARA, E-Government Act (e-Gov), and SC IT operations. The SC DDFO is designated as both the AO for SC federal systems at SC Headquarters, and the SC Enterprise AO.

The DDFO is responsible for:

1. Implementing the SC CSPP in a manner that is cost-effective and coordinated with governing bodies at the direction of S2;
2. Using a risk-based and tailored approach to delegate requirements and responsibilities for DOE policies to all SC Federal sites and SC Laboratories through the CSPP;
3. Consulting, informing, and coordinating with the DOE CIO to resolve cross-Departmental Element issues regarding the SC CSPP;
4. Providing funding resources to SC Federal sites and SC Laboratories to support an effective and efficient cybersecurity program;
5. Incorporating information security into business processes aligned to Federal and Departmental requirements and in consideration of mission needs;
6. Using bi-directional communication and reporting information flows to ensure that risk is addressed throughout the organization;

7. Establishing written procedures within the organization with clear lines of accountability that stipulate the organizational element responsible for implementing cybersecurity requirements.

1.9.3 SC Director of the Office of Information Management

The Director of the Office of Information Management serves as the SC CIO and carries out the responsibilities of CIO as required by Federal law, regulation, and policy. The SC CIO is responsible for:

1. Designating a CISO who shall carry out the CISO's responsibilities under FISMA;

2. Developing and maintaining SC's Cybersecurity Program, along with associated cybersecurity policies, procedures, and technical controls to address information security requirements;

3. Overseeing personnel with significant responsibilities for cybersecurity and ensuring that the personnel are adequately trained;

4. Assisting SC Federal sites and SC Laboratories with their cybersecurity responsibilities; and

5. Reporting to SC senior leadership on the effectiveness of the SC's Cybersecurity Program, including progress of remedial actions.

1.9.4 SC Director of the Office of Cybersecurity

The Director of the Office of Cybersecurity serves as the SC Chief Information Security Officer (CISO). The SC CISO oversees the Office of Science's Cybersecurity Program and leads SC efforts to achieve trustworthy and secure information systems as required by Federal law, regulation, and policy.

The SC CISO is responsible for:

1. Managing the overarching SC cybersecurity program;

2. Developing and executing the SC CSPP;

3. Coordinating and managing a SC-wide cybersecurity incident reporting, assessment, and response program in close coordination with existing DOE enterprise incident response reporting programs;

4. Overseeing the SC cybersecurity budget for SC Laboratories and SC Federal sites in conjunction with the SC Site AO;

5. Coordinating cybersecurity incident management with other DOE Elements, and other U.S. Government organizations as circumstances warrant;

6. Coordinating with the DOE CIO / Senior Agency Official for Privacy (SAOP) and the Chief Privacy Officer (CPO) to ensure coordination between privacy and information security programs;

7. Maintaining a register of SC's AOs, and serving as the primary liaison for cybersecurity to SC's AOs, and SC Laboratory CIOs and CISOs;

8. Coordinating and developing SC's response for all SC Federal sites or SC Laboratory cybersecurity inquiries, FISMA reporting, and other responses to Congress, DHS, and OMB;

9. Executing the duties as the SC SAO for High Value Asset (HVA) responsibilities;

10. Serving as the SC lead for information and communications technology Supply Chain Risk Management (SCRM);

11. Serving as the Subject Matter Expert (SME) point of contact for the SC CIO, the Deputy Director for Field Operations, and the Director of the Office of Science regarding cybersecurity activities; and

12. Proactively providing applicable threat information to SC Federal sites and SC Laboratories.

1.9.5 Authorizing Official

The role of the SC Site AO is served by a senior Federal official with the authority to assume responsibility and authority for the acceptance of risk for a site or organization operating information systems or employing an application or service from an external provider. SC AOs are responsible for ensuring that information systems under their purview are operating at an appropriate level of risk (i.e. risk acceptance), which should be documented and communicated to the appropriate officials.

AO responsibilities include:

1. Reviewing and approving the information security risk to organizational operations, assets, and individuals;

2. Ensuring that hosting, operations, and/or technical support of the system are available as needed; or in the case of M&O systems, providing Federal oversight of M&O;

3. Approving plans, memoranda of agreement or understanding, and Plans of Actions & Milestones (POA&Ms), and determining whether significant changes in information system configurations or operating environments require reauthorization;

4. Formally granting the Authority to Operate rating for systems;

5. Collaborate with the SC Laboratory to ensure the site digital infrastructure and services are designed and operated within the risk tolerance defined by the SC Director.

1.9.6 Authorizing Official Designated Representative (AODR)

An AODR can be appointed by an SC AO as needed to oversee the M&O cybersecurity program and coordinate day-to-day activities associated with the security authorization process. The AODR is a technical SME empowered to act on behalf of the AO for a limited set of activities. The AODR may make decisions regarding the following:

1. Authorization processes including system security plans (SSPs);
2. Approval and monitoring of implementation of POA&Ms; and
3. Assessment and/or determination of risk.

The only activities that cannot be delegated to an AODR are the authorization decision, risk acceptance, and signing of the authorization letter.

1.10 SUPPLEMENTAL GUIDANCE

In accordance with DOE O 205.1C, the SC CISO will develop supplemental guidance for the SC Site AOs' consideration to provide a standard baseline for key cybersecurity processes referenced in this document in alignment with FISMA, NIST, RMF, and CSF, as necessary.

1.11 INTEGRATED INFORMATION SECURITY AND PRIVACY DIRECTIVES

SC Federal Sites and SC Laboratories must abide by the requirements in the following DOE Directives, as applicable when incorporated into SC Laboratory contracts.

1.11.1 Department of Energy Cybersecurity Program (DOE O 205.1C)

DOE O 205.1C, *Department of Energy Cybersecurity Program,* enables the accomplishment of the Department's mission and fulfillment of Federal cybersecurity requirements while allowing Departmental Elements programmatic and operational flexibility, enhancing risk management, enabling effective implementation, delegating risk management to the lowest appropriate level, addressing roles and responsibilities, and setting standards for performance across all levels of the Department.

1.11.2 Department of Energy Privacy Program (DOE O 206.1 Chg. 1)

DOE O 206.1, *Department of Energy Privacy Program,* establishes Departmental implementation of agency statutory and regulatory requirements for privacy, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, Section 208 of the E Government Act of 2002, and OMB directives.

1.11.3 Identity, Credential, and Access Management (ICAM) (DOE O 206.2)

DOE O 206.2, *Identity, Credential, and Access Management (ICAM)*, establishes requirements and responsibilities for the DOE identity, credential, and access management program.

1.11.4 Mobile Technology Management (DOE O 203.2)

DOE O 203.2, *Mobile Technology Management,* establishes requirements for Federal mobile technology management and employee use of both government-furnished and personally owned mobile devices within DOE and NNSA. It also establishes requirements for use of User Agreements to govern mobile devices used for official duties. This order does not have a Contractor Requirement Document (CRD).

1.11.5 Information Security [Classified Information] (DOE O 471.6)

DOE O 471.6, *Information Security*, establishes requirements and responsibilities for Departmental Elements, including NNSA, to protect and control classified information as required by statutes, regulation, Executive Orders, government-wide policy directives and guidelines, and DOE policy and directives.

1.11.6 Official Travel (DOE O 550.1, Chg. 1)

DOE O 550.1 Chg. 1, *Official Travel*, supplements the Federal Travel Regulation [41 Code of Federal Regulations (CFR), Parts 300–304], which is the principal source of policy for Federal employee travel and relocation matters, and establishes DOE requirements and responsibilities governing official travel by contractor employees.

1.11.7 Unclassified Foreign Visits and Assignments Program (DOE O 142.3A, Chg. 2)

DOE O 142.3A Chg. 2, *Unclassified Foreign Visits and Assignments Program*, defines requirements to be established for unclassified foreign national access to Department of Energy (DOE) sites, information, technologies, and equipment.

1.11.8 Limited Personal Use of Government Office Equipment Including Information Technology (DOE O 203.1)

DOE O 203.1, *Limited Personal Use of Government Office Equipment Including Information Technology*, establishes requirements for employee's limited personal use of Government resources (office equipment and other resources including information technology) within the Department of Energy (DOE), including the National Nuclear Security Administration (NNSA). This directive does not include a CRD.

1.11.9 Foreign Engagements with DOE National Laboratories (DOE P 485.1A)

DOE P 485.1A, *Foreign Engagements with DOE National Laboratories* identifies the Department policy approach for international research collaboration and the

openness of the U.S. scientific community. The Department is committed to making DOE National Laboratories available to non-DOE entities, including foreign entities, provided such work is consistent with or complementary to the missions of DOE and the laboratory to which the work is to be assigned, and does not impede the laboratory's ability to successfully accomplish its DOE missions.

2 CYBERSECURITY FRAMEWORK (CSF)

SC will use the NIST Cybersecurity Framework to mature the cybersecurity programs of the SC Enterprise. The CSF provides a common taxonomy and mechanism for organizations to:

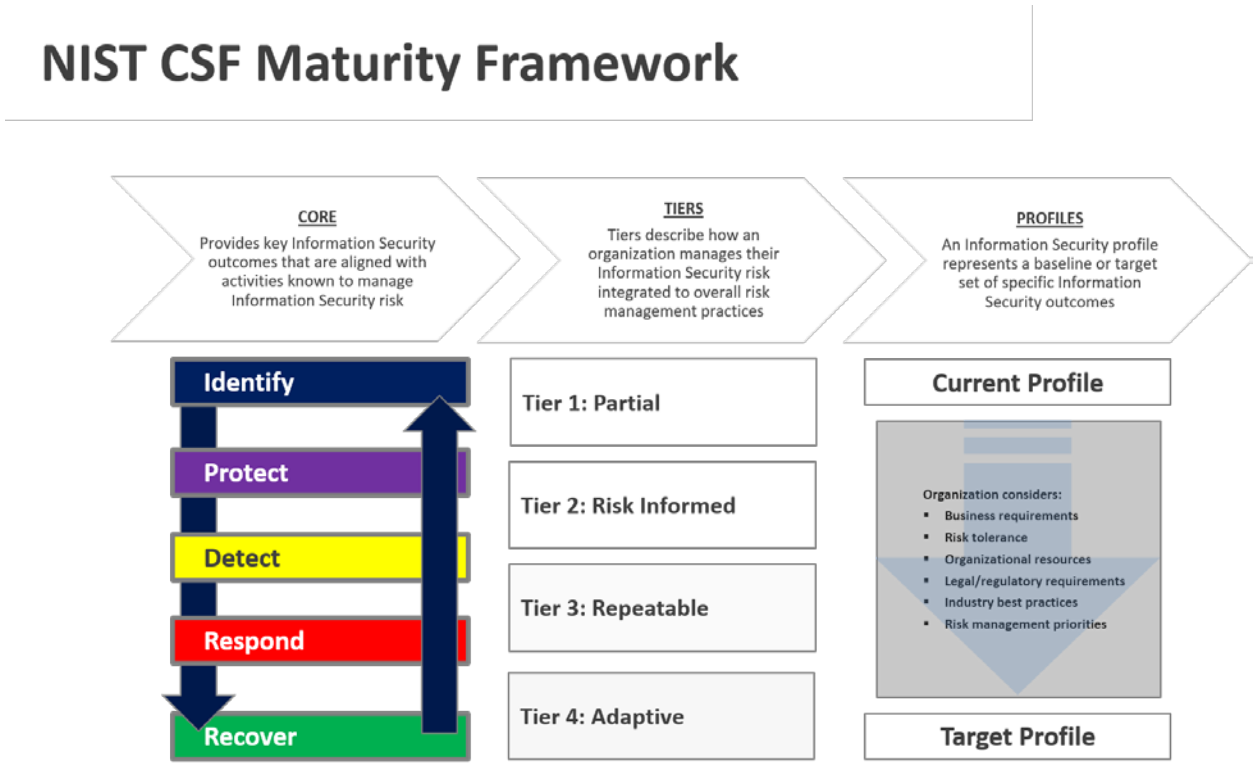
1. Describe their current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4. Assess progress toward the target state; and
5. Communicate among internal and external stakeholders about cybersecurity risk.

The Cybersecurity Framework consists of three main components: Framework Core, Implementation Tiers, and Profiles.

2.1 FRAMEWORK CORE

The Framework Core provides a set of desired cybersecurity activities and outcomes using common language. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes. The five Framework Core functions are defined as:

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.



When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

2.2 FRAMEWORK TIERS

The Framework Implementation Tiers assist organizations by providing context on how an organization views cybersecurity risk management. The Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget. The four tiers are:

- Tier 1: Partial Implementation
- Tier 2: Risk Informed
- Tier 3: Repeatable
- Tier 4: Adaptive

2.3 FRAMEWORK PROFILES

Framework Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

2.3.1 Target Profile

The cybersecurity target profile for SC systems consistent with the principles in this document will be released by the SC CISO within one year of the date of this document.

2.3.2 Current Profile

SC Federal Sites and SC Laboratories are required to maintain a cybersecurity Current Profile per NIST CSF as approved by the AO annually. To develop a Profile, the SC Federal sites or SC Laboratory will review all the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important. It can also add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the SC Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations. Implementation deadlines for this effort will be negotiated with SC Federal Sites and SC Laboratories in coordination with the release of the SC Target Profile.

2.4 GAP ANALYSIS

SC Federal sites and SC Laboratories are required to keep a current gap analysis between the SC Target Profile and their Current Profile at least annually. Implementation deadlines for this effort will be negotiated with each site in alignment with the release of the SC Target Profile and the creation of the site Current Profile.

3 ANNUAL PERFORMANCE REQUIREMENTS

3.1 CONTINUOUS IMPROVEMENT

SC Federal sites and SC Laboratories are required to demonstrate, as determined by the SC AO and SC Site AO respectively, an increased security posture year over year through any of the following:

1. Implementing new security controls,
2. Replacing older security controls with better controls,
3. Providing professional cybersecurity educational opportunities for employees,
4. Replacing legacy authentication with modern authentication,
5. Introducing new front-line defenses such as intrusion prevention systems or hardware firewalls,
6. Introducing new analytical tools and techniques,

7. Strengthening endpoint protections,

8. Introducing operational efficiency through the use of other enhancements, or

9. Achieving the same risk mitigation in a more efficient or cost-effective manner.

3.2 CYBER COLLABORATION

Extensive cyber collaboration and sharing best practices across sites takes place every day in SC and is key to maintaining a strong cyber defense. The SC CISO will enhance this collaborative environment by facilitating annual discussions among SC Laboratories to compare their cyber implementations and share best practices.

3.3 PERFORMANCE EXPECTATIONS

SC may issue cybersecurity performance expectations to SC contractors through the annual Performance Evaluation and Measurement Plan (PEMP).

4 CYBERSECURITY PROCESSES

4.1 SYSTEM INVENTORIES

SC Federal sites and SC Laboratories must maintain current system inventories in accordance with FISMA. An information system is a single or collection of computers and associated equipment with a defined logical or physical boundary that is put to a common purpose under the management of an information system owner. An information system may also consist of sub-systems which can be a single or collection of computers and associated equipment. SC Federal sites and SC Laboratories may define one or more information systems (to include national security systems). The system inventory should include identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the organization.

4.2 POA&M PROCESS

The Plan of Action & Milestone (POA&M) process is essential to managing risk at the program level. First, POA&Ms facilitate thorough documentation of the resources that are required to address risks. Second, POA&Ms allow security professionals to make incremental progress in remediation of known risks. Finally, POA&Ms give leadership operational visibility on remediation progress of known risks once resources are provided by leadership. SC Federal sites and SC Laboratories must update the DOE Cybersecurity Data Repository with the following types of POA&Ms:

- All POA&Ms for High Value Assets (HVAs);

- POA&Ms that address system and program weaknesses (to include security control test failures) that cannot be closed in less than 30 days or require significant resources to close; or

- POA&Ms that address findings and weaknesses identified by Audits, as coordinated with the SC Site AO.

The OCIO maintains the DOE Cybersecurity Data Repository in the Enterprise Cyber Governance System (ECGS). Entry to the EGCS system can be accomplished at https://cams.nnsa.energy.gov/Default.aspx. An NNSA token and an ECGS Account with password is required for access. Each POA&M must include: a designated submitter and a weakness point of contact; identification of the source of the POAM; description of the weakness; and one or more milestones for addressing the weakness.

POA&Ms identified above are required to be updated in ECGS at least quarterly, with the exception of HVA POA&Ms, which require monthly updates for open items. The status of POA&Ms and individual milestones must be covered in scheduled continuous monitoring briefings (Section 6.8) with the Authorizing Official. SC Federal sites and SC Laboratories may continue to use their own internal tracking systems that meet internal reporting criteria and requirements as part of the POA&M process.

4.3 REPORTING REQUIREMENTS

IT and Cyber related communications from outside the SC (IM, AU, etc.) will be directed to the SC Chief Information Security Officer (ciso@science.doe.gov), the SC Chief Information Officer (cio@science.doe.gov), the Science Enterprise Authorizing Official (AO) or Science Head of Contracting Activity (HCA) or appropriate federal point of contact reporting to the Science Enterprise AO or Science HCA.

All IT and cyber related communications from SC Federal sites and SC Laboratories to DOE organizations outside of SC will be coordinated through the Science AO or Science HCA and the SC Chief Information Security Officer (ciso@science.doe.gov) or the SC Chief Information Officer (cio@science.doe.gov).

4.4 MISSION IMPACT ASSESSMENTS

Mission Impact Assessments (MIA) are required upon imposition of new external requirements flowing though the SC Enterprise AO or SC CISO. Subject matter experts from both mission and cyber communities, including mission owners, assess both financial impacts and impacts on mission resiliency. The assessment should also include overarching concerns regarding SC or DOE mission, national security, and US competitive advantage. Implementation of security controls is made balancing consideration of risk reduction (including enterprise risks) vs. costs of implementation and potential disruption of mission. The mission impact assessment process must be documented in the risk management approach section of the local CSPP.

Mission impact assessments are site specific. Intimate mission insight is required to understand and illuminate impacts to the scientific mission. The MIA process should deliver a report that:

- Describes the driver that is (potentially) changing site risk posture.
- Identifies and documents the appropriate stakeholders (Mission, IT infrastructure, cybersecurity, SC Site AO).
- Identifies the potential actions to mitigate the increased risk.
- If a prescriptive technology or process is directed by the SC Enterprise AO or SC CISO, include justification for any selection of alternative risk responses.
- Captures the impact of proposed mitigation action(s) (Cost, experiment impact, collaboration impact, schedule impact, etc.).
- Is presented as a formal recommendation(s) to SC Site AO for approval.

4.5 COMPENSATORY CONTROL APPROVAL PROCESS

Where externally prescribed security controls are directed by the SC CISO, the selection of compensating controls must be approved by the SC Site AO and communicated to the SC CISO. In special circumstances of national security concern, the SC CISO may declare that compensatory controls for a particular risk must be approved by SC CISO or SC Enterprise AO.

The proposal for use of compensating controls must include the following elements:

- A Mission Impact Assessment (Section 4.4)
- An analysis comparing how the risk is managed by either existing site security controls or new alternative controls, and
- A demonstration to and approval by the SC Site AO that this alternative risk management results in a level of risk consistent with current site risk tolerance.

If a compensatory control is approved, the aforementioned documentation must be included in risk acceptance documentation that is approved by the SC Site AO.

Compensatory controls must be reviewed with the SC Site AO at least annually.

4.6 CYBERSECURITY BUDGET

The SC Chief Information Security Officer will conduct an annual budgeting process to generate budget requests for SC Federal sites and SC Laboratories, allocate funding, and to oversee associated funded projects or programs.

4.7 CYBERSECURITY ASSESSMENTS

Cybersecurity Surveys are conducted by the SC Office of Cybersecurity (SC 43.1) to provide an independent evaluation of an SC Laboratory's cyber program, to validate continuous monitoring and contractor assurance information, and to provide insight into security control implementation. These surveys are in addition to more formal assessments conducted at

each site by the DOE Office of the Inspector General (OIG) and the DOE Office of Enterprise Assessments (EA).

Cybersecurity Surveys are organized into three topical areas as applicable: Classified Cybersecurity, Telecommunications Security, and Unclassified Cybersecurity. The Classified and Unclassified Cybersecurity topics have three sub-topical areas: Program Management, Security Authorization and Risk Management, and Security Control Implementation. The Telecommunications Security Topical area is concerned with the annual review of the SC Federal sites or SC Laboratory's TEMPEST posture and observance of Red/Black separation in classified system installations.

Cybersecurity Survey results are expressed as Findings, Observations, ratings for each sub-topical and topical area, as well as an overall rating. The SC Laboratory must develop a Plan of Action and Milestones (POA&M) to address each finding. Observations are provided to identify areas that are compliant with applicable requirements but should be further evaluated for improvement. An Observation is an Opportunity for Improvement (OFI) provided to the SC Laboratory for consideration and implementation, as deemed appropriate. An Observation can also recognize a strength or positive process being implemented by the SC Laboratory. No corrective actions are needed for an Observation.

At the end of each fiscal year, the SC 43.1 Cyber Field Operations Lead reviews oversight conducted at SC Laboratories for the prior five fiscal years. The analysis considers the DOE Office of Inspector General (OIG) reviews, the DOE Office of the Inspector General full scope and partial scope reviews, and SC Cybersecurity surveys. Organizations that have received the least oversight coverage are assigned highest priority for the next fiscal year's Cybersecurity survey schedule. The goal is to conduct a survey at each SC Laboratory every three years. Reviews by the DOE Office of Inspector General and/or the Office of Enterprise Assessments may be accepted in lieu of SC Survey coverage.

4.7.1 Remediation of Findings

SC Federal sites and SC Laboratories must correct findings within 90 days unless a POA&M specifying a different time frame is approved by the SC Site AO.

5 RISK MANAGEMENT

The SC risk approach uses the Risk Management Framework (RMF) described in NIST SP 800-37R2, *Risk Management Framework for Information Systems and Organization: A System Life Cycle for Security and Privacy*. The Risk Management process requires the involvement of the entire organization, from senior leadership through the implementation of business and mission processes, to the implementation and management of information systems to support business processed.

5.1 RISK-BASED APPROACH

Due to the wide diversity of programs and missions at the Office of Science National Laboratories, it is beneficial to have a common starting point to address cyber risks across the enterprise. The unique nature and operation of each site may merit adaptation and modification in both the approach and application of requirements. However, understanding these differences across the sites and in contrast to the SC enterprise norm is important for risk acceptance and awareness.

Each SC site must have a robust risk management program to address current and emerging risks and maintain and communicate a well-founded and approved extent of acceptable risk (i.e. risk tolerance). Site risk management programs must be consistent with NIST SP 800-37 Risk Management Framework for Information Systems and Organizations. This section defines the processes for notification of new cybersecurity threats or requirements and approaches to evaluate risks against the current risk tolerance.

Notification of new cyber threats or requirements for controls that are prescribed by DOE or Federal agencies should flow through SC CISO or SC Enterprise AO per CSPP section 1.7. Notification will originate from SC CISO or the Enterprise AO to the sites and include identification of a new or modified threat or requirement. The SC CISO or Enterprise AO will provide additional insight on the threat as well as guidance on interpretation, scope and applicability of any requirements.

The outline below reflects the common approach for a SC Site AO (working with the site ISSM or equivalent) to evaluate a risk or requirement against the current risk tolerance:

For each step, the decisions and pertinent supporting information must be documented, communicated with the SC Site AO who must coordinate with the SC CISO or SC Enterprise AO.

- **Applicable**? If not applicable to site (due to mission or mission impact)
    - Local decision recorded
- **Covered**? If in the existing risk tolerance
    - Local decision recorded
- **Mitigated**? If existing controls exist that mitigate the threat or address the requirement such that risk is acceptable
    - Local decision recorded
- **Action Required**? If not in existing risk tolerance
    - Conduct mission impact assessment (CSPP Section 4.4)
    - If mission impact is not acceptable

- Document mission impact
- Then look at compensating controls
  - If effective compensating controls exist
    - Compensatory action merited?

- Site ISSM develops mitigations considering impact on mission
- Solution, cost and timeline presented to the SC Site AO
- SC Site AO concurs and presents to SC CISO
- SC funds mitigations if appropriate, or M&O seeks funding internally if required
  - Site implements mitigations
  - Over time mitigations audited
- SC Funds not provided or other funds not immediately available
  - Develop POA&M

5.2 RISK MANAGEMENT FRAMEWORK

There are seven steps to implementing the RMF:

1. Prepare to execute the RMF by establishing organization level and system level priorities for managing security and privacy risk.
2. Categorize the system and information processes, stored and transmitted based on an analysis of the impact of loss or compromise.
3. Select an initial set of security and privacy controls, tailored as needed, to reduce the risk to acceptable levels.
4. Implement the control and describe how the controls function within the system operating environment.
5. Assess the controls to determine if they are implemented correctly, operating as intended, and producing the desired outcomes in reducing risk and satisfying security and privacy requirements.
6. Obtain an Authority to Operate (ATO) for the information system based on a determination that the risk in operating the system is acceptable.
7. Monitoring the systems and the associated controls on an ongoing basis. This process includes assessing control effectiveness, documenting changes to the system and

environment, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

5.3 RISK FRAMING

Risk framing begins with an understanding of organization information, information system assets, and the processes enabled by these assets; the importance of these assets to the mission and operations; and the impacts associated with the loss of confidentiality, integrity, or availability of information or information systems. This understanding is achieved through a governance structure that is inclusive to organization elements and the maintenance of a Business Impact Analysis (BIA) for the organization. SC Federal sites and SC Laboratories categorize their information and information systems using FIPS 199 and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, or appropriate sponsor guidance for unique requirements, including DOE, non-DOE sponsors, or the local site. The SC Laboratory must also make a determination as to the presence of any national or agency critical infrastructure and identify all High Value assets that fall within the information system boundary.

5.4 RISK ASSESSMENT

SC Federal sites and SC Laboratories conduct risk assessments of information systems in accordance with NIST SP 800-30, *Guide for Conducting Risk Assessments*. The Risk Assessment is an integral part of the System Authorization Documentation and it must include a determination of risk in context of the SC Laboratory's mission, as well as residual risk to be accepted by the AO. The risk assessment process assures that cost-effective reduction strategies are applied to the environment to implement a defense posture commensurate with the risk of compromise or destruction of the information being developed, transmitted or stored. These strategies must ensure that the mission of the organization is protected, not just its information assets.

The risk assessment is:

1. Reviewed and updated at least annually and updated to address any new risk factors or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system;

2. Consistent with SC's missions, functions, directives, policies, regulations, standards, and guidance.

3. Inclusive of categorization of the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan;

4. Inclusive of the mission/business process and recovery criticality;

5. Inclusive of outage impacts and acceptable downtime;

6. Developed to address assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that supports the operations and assets of the agency;

7. Inclusive of risk due to tailoring of security controls. The risk assessment contains a clear statement of any residual risk that is being accepted by the Authorizing Official.

5.5 RISK TOLERANCE AND PRIORITIZATION

There may be different priorities associated with organizational missions and business processes that need to be factored into risk decisions, within specific elements of the organization as well as for the overall risk tolerance of the organization. Establishing the acceptable risk tolerance for the SC Laboratory involves partnership that includes the Federal Site Manager, and SC Leadership as appropriate. Subsequent risk management decisions made by the SC Federal sites and SC Laboratories should be guided by SC risk guidance and assessments of organizational impact of the spectrum of threats to information and information system assets. SC Laboratories implementing the Contractor Assurance System (CAS) should establish and implement site-specific risk tolerance according to the CAS.

The following priorities for the mitigation of cyber risk should be observed in the risk management process:

1. Risks that could impact the life, health, and safety of employees or the public.

2. Risks that could result in the compromise of Classified Information or collections of Controlled Unclassified Information that could compromise Classified Information.

3. Risks that could cause degradation of the protection of High Value Assets and national or agency critical infrastructure.

4. Risks that could cause destruction, degradation or interruption to processes, or assets or compromise of information that is important to the site mission.

5. Risks that can damage the Nation's competitive advantage, including the theft of intellectual property.

6. Risks that could result in the compromise of Controlled Unclassified Information (CUI).

7. Risks that could damage the reputation of the Nation, Department, Program Office, or site.

8. Risks that could cause the site to be out of compliance with regulations and policies.

9. Risks that could cause financial harm to the SC Laboratory.

10. Risks that could result in operational delays or outages.

As part of the Risk Assessment Process, each SC Federal Site and SC Laboratory should annually identify the impact of potential breaches, including loss of information, capabilities, and program operations; update definition of risk tolerance as part of the risk assessment; and ensure that resources and application of security controls align with the SC Federal sites or SC Laboratory's risk tolerance.

5.6 RISK REGISTER

SC Federal sites and SC Laboratories must maintain a local risk register and must also contribute to the SC Enterprise Risk Register each quarter.

5.7 INFORMATION SYSTEM SECURITY PLAN REQUIREMENTS

Each system must have an Information System Security Plan prepared in accordance with NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*. The System Security Plan is developed by the designated Information System Security Officer and the Information System Owner. The System Security Plan must address the authorization boundary of the information system, the FIPS 199 Security Categorization of the system, and the security controls implemented in the system.

5.8 AUTHORIZATION PLAN AND PROCESS

The security authorization process begins with the planning of an organization risk management framework in cooperation with the SC Federal or SC Site AO. Once the proposed system has been defined, categorized, and a risk assessment has been performed, an appropriate security control assessor or assessment team is selected and approved by the AO. An Assessment Plan is prepared and submitted to the AO for approval. This submission includes a draft information system security plan, system risk assessment, the SC Federal sites or SC Laboratory Cybersecurity Program Plan, and documentation of any common controls and privacy controls that support the information system security plan.

Upon approval of the AO, the control assessment is completed and a report documenting the results is prepared. The process may include revision to the Security Plan and Risk Assessment, as well as formulation of remediation actions and Plan of Action and Milestone items to address any modification to security controls or security control failures. A final Security Authorization Package including the following elements is submitted to the AO:

- System Security and Privacy Plan.
- The SC Federal sites or SC Laboratory Cybersecurity Program Plan and Common Control Catalog.
- The System Risk Assessment.
- Security and Privacy Control Assessment Reports.
- Plan of Action and Milestones.

- Associated plans such as Contingency Plans, Incident Response Plans, and Configuration Management Plans may be required at the discretion of the risk-accepting official.

Planning and assessment documentation may be submitted using automated tools, but those tools must provide sufficient information to allow for evaluation the details of security control implementations, as well as the tests conducted and the results. The AO, assisted by the Authorizing Official Designated Representative (AODR), and SC 43.1 staff analyzes the documentation and test results to support a determination either for further risk remediation or approval of the Security Authorization. After approval of the security authorization, any Plan of Action and Milestones (POA&M) items are monitored until completion.

Upon approval of the Security Authorization, the system is integrated into the SC Federal sites or SC Laboratory Continuous Monitoring and Continuous Authorization processes (Section 6.8). Based on the results of the Continuous Monitoring Process, the AO will document the status of the security authorization, including a statement of system performance and risk annually. Reauthorization is required for a security-significant change causing unacceptable residual risk. Security control implementation that is delayed because of infeasible or cost-prohibitive requirements is documented as a POA&M within 90 days for Federal systems, or within the period required by site contracts for contractor systems.

Significant Change or Security-Significant Change: Unless addressed through ongoing authorization activities and continuous monitoring, security-significant changes have the potential to alter the residual risk accepted by the SC Site AO, defined by the authorization package and can trigger the immediate need to assess the security state of the information system and modification of the authorization package. Organizations define security-significant changes for the information system and local environment in the site CSPP. Security-significant changes are events that can substantially raise or lower the security posture of the information systems. The following are examples of security-significant changes:

- An incident that results in a breach to the information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system;

- A newly identified, credible, information system-related threat to organizational operations and assets, individuals, other organizations, or the Nation. These are identified based on intelligence information, law enforcement information, or other credible sources of information;

- Changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, networking, or firmware, or changes in the operational environment which affect the security state of the system; or

- Changes to the organization, organizational risk management strategy, information security policy, supported missions and/or business functions, or information being processed, stored, or transmitted by the information system.

5.9 AUTHORITY TO OPERATE (ATO)

SC Federal sites and SC Laboratories may only operate systems that have a current ATO. SC Federal sites and SC Laboratories will seek an ATO for any new system or renewal of the ATO for existing systems in accordance with NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations". SC Federal sites and SC Laboratories shall assemble an authorization package and submit to their respective AO for authorization decision as indicated in Section 5.8 of this document.

6 CYBERSECURITY REQUIREMENTS

Cybersecurity requirements in Section 6 were compiled from NIST SP 800-53, DOE Directives, DOE CIO policies, and the SC Enterprise Risk Register. Utilizing the Risk Management Framework, Site AOs can coordinate with the SC CISO to formulate a risk-based and tailored approach to these requirements to meet mission needs as necessary. A complete list of references can be found in Section 8.

6.1 CYBERSECURITY POLICIES AND PROCEDURES

SC Federal sites and SC Laboratories must develop and implement a site-specific CSPP that aligns with this document. Additionally, SC Federal sites and SC Laboratories must have documented procedures and programs in place for the requirements of this document.

6.2 HIGH VALUE ASSETS

SC Federal sites and SC Laboratories must identify and protect HVAs according to OMB M-19-03: *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, and DHS BOD 18-02.

6.3 CLOUD COMPUTING REQUIREMENTS

SC Federal sites are required to use FedRAMP cloud services when available. SC Laboratories must take a risk-based approach, as detailed in Section 5.1, to using cloud services. FedRAMP compliance can be achieved through the cloud service provider either adhering to the official GSA FedRAMP program or demonstrating that they are compliant with all FedRAMP requirements. Ultimately SC is responsible for ensuring the security of their data. If only a non-FedRAMP service is available, a risk analysis must be performed on the gap between any commercial certification held by the service and the NIST security baseline. To that end, SC Federal sites and SC Laboratories are required to:

1. Analyze risk in accordance with direction from the SC Federal AO or SC Site AO for cloud applications or integrate the cloud application into the system's security plan if the cloud application is considered within the system's boundary.

2. Secure an Approval from the SC Laboratory Authorizing Official accepting the FedRAMP or Commercial certification as well as any compensating security controls and residual risks.

3. Perform a gap analysis against the element's security control baselines using the FedRAMP security control baseline of the cloud service provider. Identify additional security controls that may be required to mitigate risk, then implement and document those controls.

4. Implement two-factor authentication in accordance with DOE O 206.2 where possible.

5. Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information.

6. Based on risk, and with concurrence from the Authorizing official, review the cloud application and service provider's controls on an annual basis.

6.4 CUI REQUIREMENTS

SC Organizations process and store certain categories of unclassified information that require protection and dissemination controls mandated by statute or policy. Examples of such information that qualify as Controlled Unclassified Information (CUI) within DOE include but are not limited to Official Use Only (OUO), Export Controlled Information (ECI), Unclassified Controlled Nuclear Information (UCNI), unclassified Naval Nuclear Propulsion Information (U-NNPI), and protected Personally Identifiable Information (PII).

Per 32 CFR Part 2002 *"Controlled Unclassified Information,"* any systems that contain CUI must be categorized and protected as moderate as defined in FIPS 199, *Standards for the Security Categorization of Federal Information and Information Systems.*

6.5 RULES OF USE

Each SC Federal sites or SC Laboratory must have an acknowledgement of the "Rules of Use" by each computer user. This document must provide common rules on the appropriate use of Office of Science (SC) information and information technology resources by authorized computer users, including:

1. Computer users have a responsibility to protect and conserve Government property and shall not use such property for other than authorized purposes.

2. Computer users have no expectation of privacy in the use of SC information technology resources.

3. Computer users using SC information technology resources consent to government monitoring, interception, recording, and search of any communications or data transiting or stored on the information system or devices connected to the information system.

6.6 THREAT AWARENESS PROGRAM AND AUTOMATED INDICATOR SHARING

SC Federal sites and SC Laboratories shall stay up to date with incidents and Indicators of Compromise (IOCs) by reviewing iJC3 reports on a regular basis and participating in the iJC3 Weekly Incident Responders Conference Call. The SC CISO will release a process for collaborative threat intelligence for the SC Enterprise within 120 days of the publication of this document.

6.7 INCIDENT HANDLING AND REPORTING

Each SC Federal sites and SC Laboratory must have a Point of Contact for Incident Handling and Reporting. The POC is assigned to submit concurrent unclassified descriptions of incidents to the SC Office of Cybersecurity (SC 43.1) at scirt@science.doe.gov and the iJC3. The SC Office of Cybersecurity will then work with iJC3 on behalf of SC.

Significant or unusually persistent cybersecurity incidents must be reported to the SC Office of Cybersecurity (SC 43.1) and iJC3, including cross-contamination and privacy related incidents. An incident can be categorized as (but not limited to) attrition, cross contamination (all levels/categories), email/phishing, external/removable media, impersonation spoofing, improper usage, loss or theft, web, or other. If the incident involves Personally Identifiable Information or Private Health Information, the SC Federal sites or SC Laboratory POC should also immediately contact the SC Privacy Affairs Office (Section 6.16.1) for awareness. Specific requirements for reporting PII and PHI can be found in the Department of Energy Privacy Program Order DOE O 206.1 Chg. 1.

Any incidents that involve Classified Information, including but not limited to cross-contamination incidents, must first contact the local Incidents of Security Concern (IOSC) Manager. The SC Laboratory's Cybersecurity Point of Contact will then work with the IOSC Manager to submit information to the SC Office of Cybersecurity (SC 43.1). If a local IOSC is not assigned, the SC Federal sites or SC Laboratory should contact the Officially Designated Federal Security Authority (ODFSA).

6.8 CYBERSECURITY TESTING AND MONITORING

Contractor assurance systems and continuous monitoring are essential elements of SC assurance and oversight. The goal is to automate the sharing of continuous monitoring data wherever possible.

SC Federal sites and SC Laboratories should develop a Continuous Monitoring Plan as part of the security authorization process. The results of continuous monitoring and testing should be formally presented and briefed to the Authorizing Official in an agreed upon format. A monthly frequency is recommended, but briefings should be conducted not less than quarterly. Note: terminology from the DHS Continuous Diagnostics and Mitigation (CDM) is included parenthetically (Section 6.22). The Continuous Monitoring Plan will address indication of program performance to include performance metrics for the following program elements.

Asset Management: This element addresses management and control of hardware devices including elements of the system and devices directly accessing the internal network (HWAM), software in use on the system (SWAM), security configuration settings (CSM), and software vulnerabilities (VUL).

Identity and Access Management: This element addresses the management and control of accounts/access/managed privileges (PRIV), trust determination for users granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE).

Network Security Management: This element addresses the management of network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. This includes management of events (identification of threat vectors, detection of security violation events, classification of event impacts) (MNGEVT); operate, monitor, and improve (causal analysis of events, prioritization of security mitigation, response/recovery, notification, and post incident activity) (OMI); design and build-in security (new system, hardware, and software deployments) (DBS); boundary protection to include logical access, physical access to system components, and cryptographic protection (BOUND); and supply chain risk management (SCRM).

Data Protection Management: This element addresses the management of the protection of data. This includes data discovery/classification (DISC), data protection (PROT), data loss prevention (DLP), data breach/spillage mitigation (MIT), and information rights management (IRM).

Security Control Testing: This element addresses the testing and monitoring of security and privacy control implementation and effectiveness on risk-based frequencies.

Change Management: This element addresses the management and monitoring of changes to systems and the computing and network environment, to include corresponding changes to overall system risk.

Response to Threats: This element addresses the response to potential attacks on the information system. Metrics examined can include data from Intrusion detection and prevention systems, data from Cooperative Protection Program Sensors, data from site network access control systems, and a review of security incidents.

6.9 CONTINGENCY PLANNING

Each SC Federal sites or SC Laboratory is required to develop information system contingency plans that

1. Identify essential missions and business functions and their associated contingency requirements;

2. Addresses roles, responsibilities, recovery objectives, restoration priorities and metrics;

3. Addresses maintaining essential missions and business functions despite a disruptions, compromise, or failure; and

4. Addresses restoration without deterioration of system security controls.

Contingency planning must be supported by an analysis of mission and business processes and aligned with and coordinated with continuity of operations plans. Acceptance of risk due to assumptions or decisions made in contingency planning must be addressed in the system risk assessment. The Organization must provide role based contingency training to information system users consistent with assigned roles and responsibilities and test the system contingency plan to determine effectiveness and potential weaknesses on a frequency defined in the site CSPP or the System Security Plan (SSP).

6.10 WORKFORCE TRAINING REQUIREMENTS

SC Federal sites and SC Laboratories are required to ensure that each of their computer users is trained annually on the following:

1. Rules of Use,

2. Cybersecurity Policies and Procedures,

3. Handling CUI,

4. Protections against common methods of compromise,

5. Phishing, and

6. Incident reporting.

6.11 SUPPLY CHAIN RISK MANAGEMENT

The SC Federal sites and SC Laboratories must establish, document, and maintain a coordinated and integrated Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) program which describes the processes and risk management approach.

The SC Federal Site or SC Laboratory must:

- Develop a plan for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

- Implement the supply chain risk management plan consistently across the organization;

- Review and update the supply chain risk management plan annually or as required to address organizational changes;

- Use the SCRM resources throughout the systems life cycle and local SCRM resources where available to manage supply chain risks to the SC Federal sites or SC Laboratory systems, system components, or system services; and

- Document the selected and implemented supply chain safeguards in the SC Laboratory Cybersecurity Program Plan (CSPP) and individual system security plans and the SC Laboratories ICT SCRM Plan.

6.12 BIDIRECTIONAL REPORTING, COMMUNICATION, AND COLLABORATION

The SC Enterprise will take an open, collaborative approach to protecting our diverse scientific mission. To ensure mission-informed cybersecurity decisions are being made across the SC Enterprise, SC Laboratories will participate in monthly calls with the SC Office of Cybersecurity and with working groups and governance bodies as allowed. Additionally, SC Federal Sites and SC Laboratories will respond to data calls in a timely and accurate manner.

6.12.1 Data Calls

On a regular basis, requests for information and data calls are published by the Office of Science and other entities. Many of these are reoccurring, such as the quarterly FISMA data calls, but others may be in response to an emerging situation such as a DHS Emergency Directive. When a cybersecurity data call is received from other than SC 43.1, SC Federal sites and SC Laboratories will inform the appropriate personnel at SC so that it can be properly vetted and then distributed as necessary.

The due dates for these data collection efforts are typically a day prior to the published dates so SC has time to review the responses to ensure accuracy and consistency in the responses from the various sites. Extension requests can be coordinated as necessary if there are issues in compiling the necessary data for the responses. If there is a situation where the data is not available, SC Federal sites and SC Laboratories will coordinate as early as possible with SC 43.1 in order to ensure the best data possible is made available to the requesting entity.

6.12.2 Technical Strategy Cell

The SC CISO will convene a Technical Strategy Cell (TSC) to serve as a formal body of trusted advisors to leadership across the SC Enterprise upon request. The Technical Strategy Cell has no formal decision-making authority but instead serves as a peer-review board of trusted advisors and will provide concurrence, non-concurrence, and/or technical recommendations upon request. The TSC will not alter the relationship between or responsibilities of the AOs or SC Federal sites or SC Laboratories. AOs are not required to use the TSC or to implement the TSC's recommendations.

6.12.3 Warning Banner

The SC Federal sites or SC Laboratory will establish a warning banner that requires unclassified endpoints to display a system use notification (e.g., Warning Banner) at login and, if possible, require users to electronically acknowledge the warning (such as clicking on "OK" or "I agree" button to proceed). The warning banner must cover the following in substance:

- That by using the account or the information system, or connecting any devices to the information system, the user acknowledges, understands and consents to certain identified actions;
- The user acknowledges, understands and consents to the fact that the user has no reasonable expectation of privacy regarding communications or data transiting or stored on the information system or devices connected to the information system;
- The user acknowledges, understands and consents to the fact that at any time and for any official purpose, the government may monitor, intercept, record, and search any communications or data transiting or stored on the information system or devices connected to the information system; and
- The user acknowledges and understands and consents to the fact that any communications or data transiting or stored on the information system or devices connected to the information system may be used or disclosed for any official purpose, including to law enforcement or other government agencies, as deemed appropriate by DOE or as mandated by law.

The SC Federal sites or SC Laboratory will establish a warning banner that will display a warning banner system use notification to users before granting access to the system that provides privacy and security notices consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

For systems not accessed by the general public, the warning banner shall state that:

- Users are accessing a U.S. Government system;
- System usage may be monitored, recorded, and subject to audit;
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
- Use of the system indicates consent to monitoring and recording;

The notification message or banner must stay on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

For publicly accessible systems:

- Display system requirements for use before granting further access to the publicly accessible system;
- Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
- Include a description of the authorized uses of the system.

See DOE O 205.1C and the latest revision of NIST SP 800-53 for additional recommendations or supplemental guidance. Text for a sample DOE warning banner that has been reviewed by the DOE General Counsel can be obtained by contacting circ@jc3.doe.gov.

6.13 MEDIA CONTROL

Unauthorized use of removable media for storing, transporting and transferring data may provide an entry point for introduction of security exploitations. Additionally, use of removable media may inadvertently move sensitive data outside the enterprise network and/or the physical premises where it can potentially be accessed by unauthorized persons. Minimum security standards are defined for all users with business requirements to connect removable media to any infrastructure within DOE's internal network(s).

SC Laboratories must take a risk-based approach (as defined in Section 5.1) to the risks associated with Removeable Media per the DOE ITC memo ITC-18-03.

SC Federal sites must:

1. Use removable media that is DOE government furnished equipment (GFE) or DOE authorized removable media when storing, transporting or transferring information on DOE-owned and controlled systems. DOE GFE is property acquired by the government and provided to Federal employees and contractor support personnel for work. DOE authorized removable media is removable media that is property vetted, approved by the government, meets minimum security standards, and can be verified as procured from trusted sources.
2. Use Federal Information Processing Standard (FIPS) Publication 140-2 encryption compliant removable media hardware and/or software when storing, transporting or transferring all CUI or PII data: The FIPS Publications 140-2, Security Requirements for Cryptographic Modules, is a government computer security standard used to accredit cryptographic modules. Federal agencies and departments can validate hardware and/or software encryption certification they want to use by the FIPS 140-2 standard.

3. Protect all CUI in compliance with DOE Manual 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*; which covers the steps to minimize the risk of access by unauthorized persons.

4. Protect, store, transport and transfer PII on DOE-approved and/or DOE-furnished removable media and DOE owned equipment and systems only in accordance with the "*Safeguarding Personally Identifiable Information (PII)*" document at the following URL: https://intranet.osc.doe.gov/sites/it/Pages/Safeguarding-PII-Policy.asp. This document states "OMB M06-16 states that in instances where PII is transported or stored at a remote site, implement at least NIST SP800-53 moderate level security controls ensuring that information is transported only in encrypted form."

5. This policy does not include the use of removable media for classified information or classified systems. The Safeguards and Security program provides all security policy for classified information handling.

6.14 AUTHENTICATION REQUIREMENTS

6.14.1 Multifactor Authentication

SC Laboratories must require Multifactor Authentication (MFA) for the following types of access, except for those exclusions listed in Appendix A

- Standard user access.
- Privileged access.
- Remote access to a SC Federal sites or SC Laboratory network from the Internet.
- Access to government email accounts from the Internet.

SC Laboratories must take a Risk-Based Approach (Section 5.1) to implement MFA for any other accounts not listed above.

Details of SC's approach to MFA implementation requirements can be found in Appendix A.

6.14.2 Passwords

This section applies to devices that cannot use Personal Identity Verification (PIV) cards or approved hardware/software-based tokens and temporary password issuance. Devices covered by this policy include but are not limited to government provided Blackberries, iPhones, Microsoft Windows, Android devices and tablets used by SC customers to access Department of Energy resources.

The Authorizing Official also has the authority to establish Standard Operating Procedures (SOPs) and management practices to improve the effectiveness and efficiency of programs and operations per DOE Order 205.1C or may delegate this

authority. SC Federal sites and SC Laboratories must define a password policy in accordance with the SC Federal or SC Laboratory RMF.

6.15 PRIVACY

6.15.1 Privacy Affairs Office (PAO)

The subject matter experts assigned in the SC Offices of General Counsel as Privacy Officers are a critical resource in ensuring that the cybersecurity requirements to safeguarding personal sensitive data and should be involved in Privacy Impact Assessments (PIA), privacy-related data calls, and breaches that impact PII or PHI.

Privacy controls are addressed in the Privacy Program Plan and Privacy Continuous Monitoring Plan developed by the DOE Privacy Management and Compliance Office and are not reproduced in this document. For assistance in this area, please contact the SC Offices of General Counsel located in Lemont, IL and Oak Ridge, TN and their respective FOIA/Privacy Officers.

6.15.2 Personally Identifiable Information (PII)

The term *Personally Identifiable Information* (PII) as defined in OMB Memorandum M-17-12 refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source that, when combined with other available information, could be used to identify an individual.

6.15.3 Protected Health Information (PHI)

Protected Health Information, or PHI, is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.

6.15.4 Privacy Impact Assessments (PIA)

All applicable unclassified information systems shall have a Privacy Impact Assessment (PIA) approved by the Senior Agency Official for Privacy (SAOP) or designated official. PIAs must be reviewed annually and updated as needed.

6.15.5 Privacy Act Systems of Record (SOR)

Information collected under the Privacy Act must be stored in a Privacy Act System of Records (SOR). The Privacy Act requires agencies to publish a System of Records Notice (SORN) in the Federal Register and report to Congress when a new SOR is proposed or significant changes are made to a previously established system.

6.15.6 Privacy Breach Notifications

Upon a finding of a suspected or confirmed data breach of PII in printed, verbal, or electronic form, DOE employees must ensure that the breach is IMMEDIATELY reported to both the local Privacy Act Officer (PAO) and/or Privacy Point of Contact (PPOC) AND to the Integrated Joint Cybersecurity Command Center (iJC3) at 866-941-2472 (or via email to circ@jc3.doe.gov). The Office of Science Incident Response Team (SCIRT) shall be contacted concurrently with the above notifications via email at scirt@science.doe.gov per Section 6.7.

PII, regardless of whether it is in paper or electronic form, must be protected from unauthorized access or disclosure throughout its lifecycle. DOE employees and contractors shall limit the use of PII to only that information which is specifically needed to carry out their duties. Review of PII and PHI holdings will be accomplished annually to ensure that the use of these types of information are minimized and documented.

6.16 CYBER HYGEINE REQUIREMENTS

SC Federal sites and SC Laboratories can reduce the risk of a successful attack by layering security defenses using a Defense In Depth (DID) approach. By taking a proactive approach and managing risk with diverse defensive strategies, attackers might be thwarted even if they are able to compromise one or more layers of defense. Incorporating layered security mechanisms requires an attacker to circumvent each mechanism to gain access to a digital asset. SC Federal sites and SC Laboratories are required to employ defense in depth in the protection of their systems and networks at the perimeter, endpoint, and in data protections at a minimum, as described below.

6.16.1 Endpoint Protections

An endpoint is a GFE device or node connected to a network that generates, forwards, or receives communications. Endpoint security configuration baselines must be established, documented, and monitored for risk mitigation and cost effectiveness on a scheduled timeframe. At a minimum, endpoints must be protected with anti-virus, anti-malware, and regularly scheduled patching.

6.16.2 Perimeter Protections

SC Federal sites and SC Laboratories must proactively deny all incoming traffic (Default Deny) unless explicitly allowed and have an isolated DMZ network for

services available to the Internet. This applies to all networked devices including user devices, servers, routers, switches, encryptors, etc. This can be managed by a firewall, or by a firewall and an Intrusion Prevention System (IPS), but not with an IPS alone. Additionally, SC Federal sites and SC Laboratories should explore the use of network segmentation to protect systems and data.

6.16.3 Data Protections

To protect against ransomware and other destructive attacks, SC Federal sites and SC Laboratories must backup mission-essential data either with offline storage or immutable backup storage. SC Federal sites and SC Laboratories must use a Risk-Based Approach (Section 5.1) to backing up programmatic and business information with the potential for and consequences of loss disclosed in the system risk assessment.

6.16.4 Mobile Device Protections

All GFE mobile devices (including but not limited to laptops, phones, and tablets) that leave the perimeter of an SC office or site must have FIPS 140-2 compliant Full Disk Encryption (FDE) or a containerized encryption solution. All GFE phones and tablets must operate under enterprise-level mobile device management that includes at a minimum the ability to remotely wipe data from the device. SC Laboratories must take a Risk-Based Approach (Section 5.1) for protection of BYOD that connect to anything other than a guest network.

6.16.5 Vulnerability Remediation

SC Federal sites and SC Laboratories shall have a vulnerability discovery and remediation plan that addresses risk remediation, time to remediate, residual risk, compensating controls when necessary, and cost. This plan shall address system vulnerability and include a vulnerability scanning methodology and scanning frequency. The vulnerability remediation plan shall be agreed on between the SC Laboratory and the SC Site AO and be transparent up to the SC CISO.

Critical vulnerabilities must be remediated within 15 days of discovery. High vulnerabilities must be remediated within 30 days of discovery.

6.16.6 Network Traffic Monitoring

SC Laboratories must take a Risk-Based Approach (section 5.1) to implementing network traffic monitoring with alert capability at the network perimeter access points and strategic points on the internal network.

6.17 ANTI-PHISHING

SC Federal sites and SC Laboratories must perform anti-phishing exercises each quarter.

6.18 EMAIL SECURITY

SC Federal sites and SC Laboratories must ensure the following.

- All internet-facing mail servers to offer STARTTLS, and
- All second-level agency domains to have valid SPF/DMARC records, with at minimum a DMARC policy of “p=none” and at least one address defined as a recipient of aggregate and/or failure reports.
- Secure Sockets Layer (SSL)v2 and SSLv3 are disabled on mail servers,
- 3DES and RC4 ciphers are disabled on mail servers, and
- DMARC policy of “reject” for all second-level domains and mail-sending hosts.

6.19 WEB SECURITY

SC Federal sites and SC Laboratories must ensure the following.

- All publicly accessible Federal websites and web services provide service through a secure connection,
- SSLv2 and SSLv3 are disabled on web servers, and
- 3DES and RC4 ciphers are disabled on web servers.
- Identify and provide a list of second-level domains that can be HSTS preloaded, for which HTTPS will be enforced for all subdomains.

6.20 ICS REQUIREMENTS

Industrial Control Systems (ICS) encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

All SC Laboratories will have an ICS risk management plan per Section 5.1 prioritizing personnel safety and ICS availability per Section 5.3, addressing:

- Discovery and inventory of all ICS systems and identification of system criticality and risk
- Security and architectural strategy taking into consideration segmentation from internet accessible networks, redundancy, fault tolerance and authentication to systems and devices
- Physical security of networks and devices

- Identification, detection, response, and recovery for incidents and security events
- Security control implementation and testing frequency for risk mitigation and cost effectiveness

6.21 CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM (CDM)

SC Federal sites and SC Laboratories must participate in the DHS Continuous Diagnostics and Mitigation (CDM) program, at the direction of the SC Chief Information Security Officer.

6.22 VULNERABILITY DISCLOSURE PROGRAM (VDP)

SC Federal sites and SC Laboratories must participate in the Vulnerability Disclosure Program (VDP), at the direction of the SC Chief Information Security Officer.

6.23 DATA SHARING AND BIG DATA PLATFORM (BDP)

SC Federal sites and SC Laboratories shall participate in the Data Sharing effort with the DOE OCIO, at the direction of the SC Chief Information Security Officer.

7 IMPLEMENTATION

In coordination with the SC site office, each SC Laboratory must present a gap analysis with the requirements in this document to the SC Chief Information Security Officer along with a risk-based prioritization of gaps, an implementation plan on how to come into compliance with this CSPP, and any necessary one-time or baseline funding requests no later than June 30, 2021. Each SC Federal site and SC Laboratory must submit an AO-approved site CSPP to the SC Office of Cybersecurity no later than September 30, 2021. Site CSPPs must align with the SC CSPP and be updated and renewed annually. Each SC Laboratory must track the progress of their implementation plan with the SC Site AO and provide quarterly reports to the SC CISO until they are fully compliant with this CSPP.

References

1. 2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII) https://www.gsa.gov/directive/gsa-rules-of-behavior-for-handling-personally-identifiable-information-%28pii%29-

2. 44 U.S.C. § 3541 et seq., Federal Information Security Management Act of 2002 (FISMA) 44 U.S.C. § 3542(2) (A), https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

3. Atomic Energy Act, 42 U.S.C. § 2011 et seq, https://www.govinfo.gov/content/pkg/USCODE-2010-title42/html/USCODE-2010-title42-chap23-divsnA.htm

4. Clinger-Cohen Act of 1996, Title 40, https://www.govinfo.gov/content/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf

5. CNSS Policy 26, National Policy on Reducing the Risk of Removable Media for National Security Systems (FOUO), http://www.cnss.gov/CNSS/issuances/Policies.cfm

6. CNSSI 1254, Risk Management Framework Documentation, Data Element Standards, and Reciprocity Processes for National Security Systems, http://www.cnss.gov/CNSS/issuances/Instructions.cfm

7. DHS BOD 18-02 Securing High Value Assets, https://cyber.dhs.gov/directives/

8. DHS BOD 19-02 Vulnerability Remediation Requirements, https://cyber.dhs.gov/directives/

9. DOE CISO Amplification Guidance (04/03/2020), FISMA Inventory Methodology.

10. DOE ITC 18-01, Anti-Phishing Security Defenses, https://powerpedia.energy.gov/wiki/File:Anti-Phishing_Security_Defenses_(DOE_ITC_18-01).pdf

11. DOE ITC 18-02, Remote Access, https://powerpedia.energy.gov/wiki/File:Remote_Access_Security_(DOE_ITC_18-02).pdf

12. DOE ITC 18-03, Removable Media Security, https://powerpedia.energy.gov/w/images/1/13/DOE_ITC_18-03_-_Removable_Media.pdf

13. DOE ITC 18-04, Social Media Security, https://powerpedia.energy.gov/wiki/File:DOE_ITC_18-04_-_Social_Media.pdf

14. DOE Manual 471.3-1 Chg. 1 (Admin Chg.) Manual for Identifying and Protecting Official Use Only Information, https://www.directives.doe.gov/directives-documents/400-series/0471.3-DManual-1-admchg1/@@images/file

15. DOE Order 150.1A, Continuity Programs, https://www.directives.doe.gov/directives-documents/100-series/0150.1-BOrder-a/@@images/file

16. DOE Order 200.1A, Information Technology Management, https://www.directives.doe.gov/directives-documents/200-series/0200.1-BOrder-a-chg1-minchg/@@images/file

17. DOE Order 203.1, Limited Personal Use of Government Office Equipment Including Information Technology, https://www.directives.doe.gov/directives-documents/200-series/0203.1-BOrder/@@images/file

18. DOE Order 203.2, Mobile Technology Management, https://www.directives.doe.gov/directives-documents/200-series/0203.2-BOrder/@@images/file

19. DOE Order 205.1C Department of Energy Cybersecurity Program, https://www.directives.doe.gov/directives-documents/200-series/0205.1-BOrder-c/@@images/file

20. DOE Order 206.1, Department of Energy Privacy Program, https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder-chg1-minchg/@@images/file

21. DOE Order 206.2, Identity, Credential, and Access Management (ICAM), https://www.directives.doe.gov/directives-documents/200-series/0206.2-BOrder/@@images/file

22. DOE Order 241.1B Chg. 1 (Admin Chg.), Scientific and Technical Information Management, https://www.directives.doe.gov/directives-documents/200-series/0241.1-BOrder-b-chg1-adminchg/@@images/file

23. DOE Order 470.4B, Safeguards and Security Program, https://www.directives.doe.gov/directives-documents/400-series/0470.4-BOrder-B-Chg2-MinChg/@@images/file

24. DOE Order 471.1B Identification and Protection of Unclassified Controlled Nuclear Information, https://www.directives.doe.gov/directives-documents/400-series/0471.1-BOrder-b/@@images/file

25. DOE Order 471.3, Identifying and Protecting Official Use Only Information, https://www.directives.doe.gov/directives-documents/400-series/0471.3-BOrder-admchg1/@@images/file

26. DOE Order 471.6, Information Security, https://www.directives.doe.gov/directives-documents/400-series/0471.6-BOrder-admchg3/@@images/file

27. DOE Order 472.2, Personnel Security, https://www.directives.doe.gov/directives-documents/400-series/0472.2-BOrder-chg1-pgchg/@@images/file

28. DOE Order 550.1, Official Foreign Travel, https://www.directives.doe.gov/directives-documents/500-series/0550.1-border-chg1-ltdchg/@@images/file

29. DOE Policy 485.1A, Foreign Engagements with DOE National Laboratories, https://www.directives.doe.gov/directives-documents/400-series/0485.1-apolicy-a/@@images/file

30. DOE Policy 413.1, Program and Project Management Policy for the Planning, Programming, Budgeting, and Acquisition of Capital Assets, https://www.directives.doe.gov/directives-documents/400-series/0413.1-APolicy/@@images/file

31. E-Government Act of 2002 Pub L 107-347, 116 Stat 2899, https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

32. Executive Order 13526, Classified National Security Information (Dec. 29, 2009), https://www.govinfo.gov/content/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf

33. FIPS 140-2 Security Requirements for Cryptographic Modules. https://csrc.nist.gov/publications/detail/fips/140/2/final

34. FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

35. Functions, Responsibilities, and Authorities (FRA) for Safety, Security, and National Environmental Policy Act (NEPA) Management, Office of Science, October 2019.

36. Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors, https://www.govinfo.gov/content/pkg/PPP-2004-book2/pdf/PPP-2004-book2-doc-pg1765.pdf

37. NIST Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

38. NIST SP 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-116r1.pdf

39. NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

40. NIST SP 800-160 Vol 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

41. NIST SP 800-160 Vol. 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

42. NIST SP 800-171 rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, February 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

43. NIST SP 800-18 rev 1, Guide for Developing Security Plans for Federal Information systems, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

44. NIST SP 800-183, Network of 'Things', https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

45. NIST SP 800-30, Guide for Conducting Risk Assessments, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

46. NIST SP 800-34 rev 1, Contingency Planning Guide for Federal Information Systems, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

47. NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

48. NIST SP 800-39 Managing Information Security Risk, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

49. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

50. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations (Draft), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5-draft.pdf

51. NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

52. NIST SP 800-63-3 Digital Identity Guidelines, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

53. NIST SP 800-63-3A Digital Identity Guidelines: Enrollment and Identity Proofing, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf

54. NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

55. NIST SP 800-88, Guidelines for Media Sanitization, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917935

56. OMB Circular No. A-11, Preparation, Submission and Execution of the Budget, https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

57. OMB Circular No. A-130, Managing Information as a Strategic Resource, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

58. OMB M-04-04, E-Authentication Guidance for Federal Agencies, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf

59. OMB M-05-24, Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf

60. OMB M-06-16, Protection of Sensitive Agency Information, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2006/m06-16.pdf

61. OMB Memorandum M-07-1616, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

62. OMB M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-11.pdf

63. OMB M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

64. OMB M-19-03: Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program, https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

65. OMB Memorandum for CIOs, Security Authorization of Information Systems in Cloud Computing Environments (2012), https://www.fismacenter.com/fedrampmemo.pdf

66. SC Lab Appraisal Process, https://science.osti.gov/lp/Laboratory-Appraisal-Process

67. US-Cert Cyber Threat Source Descriptions, https://www.us-cert.gov/ics/content/cyber-threat-source-descriptions

Appendix A SC Multifactor Authentication Approach

The Office of Science has a statutory requirement to maintain and extend Multifactor Authentication (MFA) in the federal and open science environments. The objectives for MFA in SC apply to network accounts on unclassified systems that employ compliant MFA, for Federal and contractor (including M&O) users.

A.1 APPROACH

The Science labs are specifically charged with making most of the mission research-related information public. This scope of open or to-be-published information excludes information that requires protection such as personal, national security, and company-proprietary information. The research programs in the Office of Science programs in particular have a requirement to publish the results of open scientific research. One embodiment of these goals is the operation of numerous User Facilities that welcome guest users, industry partners, and visiting scientists from around the country and internationally.

Because of these diverse missions and associated operating environments, the Science and Energy programs and laboratories operate complex network architectures that, in varying ways, segregate different levels of operational and information sensitivities, and the associated users of those capabilities.

SC has employed a risk-based approach to implementing Multifactor Authentication that is specific to the needs of its unique environment and makes use of enterprise solutions. Based on this MFA guidance and other direction provided by DOE and the Program Office, the Authorizing Official (AO) is responsible for interpreting the MFA requirements; tracking, resolving, or escalating any issues; and evaluating the implementation of the requirements.

A.2 SCOPE

The scope of the MFA effort is privileged network user accounts, standard network user accounts, and internet-accessible email accounts (note that an individual user may have multiple network user accounts, some privileged and some standard network accounts). Local accounts, application accounts, accounts associated with non-person entities, disaster/recovery scenarios, and access to mobile devices are out of scope.

SC operates some infrastructures where AAL3/IAL3 MFA implementation is not appropriate. For such systems, each site will provide an exception based on mission requirements and document it in the system ATO. This will replace the previous DOE Exception Process with a locally managed and documented process that will be reviewed during cybersecurity surveys.

The scope of the SC MFA Guidance is described through discussion of types of credentials and the user populations.

A.3 TYPES OF CREDENTIALS

OMB Memorandum-05-24 (M-05-24) requires the use of an IAL3/AAL3 Credential, for example Personal Identity Verification (PIV) credential, as outlined in Homeland Security Presidential Directive 12 (HSPD-

12). DOE O 206.2 mandates issuance and use of IAL3/AAL3 credentials for all Federal employees, cleared contractors, and contractors at Headquarters locations. Authorizing Officials are permitted to make a risk-based determination to employ an alternative strong MFA solution. Credentials used for logical access should be IAL3/AAL3 unless supported by an exception described below.

For uncleared contractors at field sites who currently do not have a HSPD-12/PIV credential, IAL3/AAL3 credentials such as PIV-Interoperability (PIV-I), Commercial Identity Verification (CIV; also referred to as PIV-C), YubiKey, or comparable solution can be issued as an acceptable alternative, based on a risk management decision by the Authorizing Official. Per NIST SP 800-63-2, an IAL3/AAL3 credential must include hardware module certification; identity proofing; and processes for credential issuance, management, and revocation.

A.4 USER POPULATIONS

Given SC's complex ecosystem, it is necessary to clearly define the universe of users. The first distinction is between privileged network user accounts and standard network user accounts, as defined in NIST publications.

A.4.1 Guidance on privileged network users:

Privileged network users are defined by SC as users who are authorized (and therefore trusted) to perform security-relevant functions that standard network users are not authorized to perform (NIST SP 800-53). Additional guidance on privileged network users follows:

- The privileges identified as "security-relevant functions" are specified and approved based on the Risk Impact Level of the associated Information System.
- The locus of the determination of "security-relevant functions" is at the NIST System (i.e., Enclave, Grouping, Major Application, and General Support System) level.
- Privileged network users are identified by the scope of security-relevant functions they are allowed to perform.
- Generally, privileged network users should have unusual levels of security-function related privilege compared to general users at the site.

Representative examples of privileged network users:

- Domain administrator or organizational unit administrator.
- Database or application administrator (where indicated by risk).
- System administrators (where indicated by risk).
- Workstation administrators (where indicated by risk).
- Firewall administrators.

- Network infrastructure device/system/appliance administrators.

A.4.2 Guidance on standard network users:

Standard network users are defined by the Department as organizational users who are not privileged network users (NIST SP 800-53). Organizational users are defined as organizational employees or individuals the organization deems to have equivalent status of employees including, for example, contractors, guest researchers, and individuals detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.

Representative examples of standard network users:

General purpose business system users in office computing environments.

A.4.3 Guidance on user accounts:

There is a distinction between users ***as people*** and ***user accounts***. Every account with different privileges or login credentials is considered a separate user account, and it is at the user-account level that MFA is applied and counted. Authentication to a standard network user account cannot be used to meet the requirement for IAL3/AAL3 authentication to the same user's privileged network user account.

- A single user who logs onto multiple computing systems with the same account counts as a single user account.

- A user account that logs onto both excluded FIPS 199 Low Confidentiality/Low Integrity/Low Availability systems and non-excluded systems only needs to use MFA for the non-excluded systems.

A.4.4 Network users' populations

These network user accounts can be separated into organizational and non-organizational users. The users can be defined further as in scope or out of scope, as defined by Scope Boundaries.

A.5 EXEMPTIONS

Exemptions are categories of users and/or systems that are not part of the scope of the MFA effort.

Exemptions were outlined in OMB Memorandum-05-24 (M-05-24) issued on August 5, 2005:

- Occasional visitors to Federal facilities to whom an agency would issue temporary identification.

- Individuals under contract to a department or agency, requiring only intermittent access to Federally Controlled Facilities.

A.6 EXCLUSIONS

Exclusions are categories of users and/or systems are not considered in scope due to the nature of their interaction with the DOE network. For example, researchers remotely collaborating as users of DOE experimental facilities are not included in the scope of the MFAIA. There are other very specific categories of users and systems that are excluded as a matter of policy.

Additional guidance on standard network users follows:

- The scope of standard network users includes only organizational users unless the mission specific environment necessitates a different approach. For example, R&D environments typically have many classes of collaborators, but only those with employee-like privileges should be considered organizational users based on local risk-assessment of those privileges.
- Exclude accounts on systems in Low/Low/Low Risk Impact Information Systems that cannot be used to access and/or have no special trust relationship with Moderate Risk Impact Systems.
- Exclude accounts that are not interactive console-type users (e.g., shell, remote desktop) on traditional organizationally owned computing endpoints such as general-purpose computing workstations, laptops, and servers.
- Exclude local and special purpose accounts which provide no security-related functionality if internal controls exist to mitigate the risks associated with these processes and if logically or physically segregated from other institutional systems.
- Exclude process (service) and system accounts (computer to computer/application to application accounts) if internal controls exist to mitigate the risks associated with these processes.
- Exclude accounts on experimental support systems or industrial control systems if logically or physically segregated from other systems.
- Exclude accounts on collaborative systems designed and architected to provide collaboration resources to non-organizational users, regardless of whether the user is organizational or non-organizational if logically or physically segregated from other systems (Departmental Elements to identify thresholds for segregation based on risk).
- Exclude accounts within FIPS 199 Low/Low/Low information systems designed and architected for scientific collaboration with the external, non-organizational user from the scientific community if logically or physically segregated from other systems (Departmental Elements to identify thresholds for segregation based on risk).
- Exclude accounts within FIPS 199 Low/Low/Low information systems if those systems have no trust relationships with other information systems at the site (e.g., they are “Starbucks Wi-Fi Like” with regards to other site systems).

A.7 EXCEPTIONS

Exceptions are categories of users and/or systems where compensatory security controls are implemented as an alternative to a IAL3/AAL3 solution to maintain an acceptable level of risk, in cases where use of IAL3/AAL3 solutions would impact the mission, are not technically feasible, would increase risk, or fall into certain specific risk-based categories. The expectation is that excepted systems and users will generally use an alternative strong MFA solution (equivalent to IAL2/AAL2 or better) along with other controls or architectural considerations.

Exceptions rely on risk management reviews by technical experts and acceptance of residual risk by the Authorizing Official and must be documented and approved in writing as part of the ATO and Risk Management process.

Exception types include:

- Type 1: Break Mission Exceptions
- Type 2: Technically Incompatible Exceptions
- Type 3: Increased Risk Exceptions
- Type 4: Categorical Exceptions

Excepted systems and network user accounts will be considered on a case-by-case basis and will be closely monitored and managed by the AO. MFA implementation for excepted systems must use compensating security controls to maintain an acceptable level of risk and be closely monitored to ensure that those controls have been effectively put in place. The mitigation approaches must include robust risk management strategies tailored to the specific use cases. The exception review process will ensure that risks are reduced to acceptable levels mandated by NIST SP 800-37, so the overall risk levels can be effectively managed and not be increased.

A.8 GOVERNANCE

Per DOE O 205.1C, site Authorizing Officials (AOs) ensure full compliance with the standards set forth in NIST SP 800-63/800-63-1/800-63-2 and that the sites demonstrate appropriate assurance practices using existing risk management documentation and procedures. Additionally, the AO is responsible for addressing risks and threats outlined in NIST SP 800-63 as well as any additional identified risks.