Security Policy for Columbus Collaboratory

NOT FOR DISTRIBUTION

Table of Contents

Document Management

Approvals

Reviewed and Approved	Vice President of Delivery and Experience
Reviewed and Submitted for Approval	Vice President of Security Innovation
Submitted for Review	William Yang, CISSP wyang@jasadvisors.com
Submitted for Comment	William Yang, CISSP wyang@jasadvisors.com September 6, 2016

Revision Control

2016-10-26	wyang@jasadvisors.com	Update to reconcile all submitted edits and provide clarification as needed from comments received by 10/17. Due to the number and scope of those changes, the modifications have not been itemized.
2016-09-15	wyang@jasadvisors.com	Updated AC-7 baseline procedures; updated org chart and roles and responsibilities; included several questions and answers in comments; general cleanup.
2016-09-06	wyang@jasadvisors.com	Adjusted to BASE level assurance from MODERATE.
2017-05-24	ltenerove@cbuscollaboratory.com	Added title page and header.

Introduction

The Columbus Collaboratory, LLC (the "Collaboratory" or the "Company") is committed to protecting its employees, partners, and itself from both intentional and unintentional damaging acts. Effective information security is a team effort involving the participation and support of every person or organization that interacts with non-public data or system in the custody, owned or operated by the Collaboratory ("user"). Therefore, it is the responsibility of every user and participant to know and understand how to conduct their activities in conformance with this policy. Because the Collaboratory is in possession of data entrusted to the Collaboratory by third parties with the expectation that the data will be protected appropriately, this policy will provide appropriate guidance as to the minimum levels of security that can be expected.

Protecting company data and the systems that collect, process, and maintain this information requires the application of security controls to ensure accountability, availability, integrity, and confidentiality of data, systems and processes.

- **Confidentiality** addresses the preservation of restrictions on information access and disclosure so that access is limited to authorized users and services.
- **Integrity** addresses the concern that sensitive data has not been modified or deleted in an unauthorized, unintentional or undetected manner.
- **Availability** addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against the possibility of unauthorized access to, alteration, disclosure, loss of access or control, or destruction of data and systems—regardless of whether the event is intentional or unintentional.

This document is intended to create an information security framework for the Collaboratory that is consistent with the requirements and guidance of the National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 4.

Scope and Applicability

This policy and the associated procedures, standards and guidelines apply to all Collaboratory data, systems, activities, and assets owned, leased, controlled or used by the Collaboratory, its agents, contractors or other business partners on behalf of the Collaboratory. These policies, standards, procedures and guidelines apply to all Collaboratory employees, contractors, sub-contractors, and their respective facilities supporting Collaboratory business operations, wherever Collaboratory data is stored or processed, including any third party contracted by Collaboratory to handle, process, transmit, store or dispose of Collaboratory data.

Some policies are explicitly stated for persons with a specific role (e.g. a system manager); otherwise, all personnel supporting Collaboratory business functions shall comply with the policies. This policy may

through localized addendum be made more restrictive, strict, or comprehensive policies applicable on a subset of Collaboratory functions and data, but will serve as the minimum baseline for all Collaboratory data, systems, activities, and assets.

Security controls identified as [ENHANCED] are not mandatory control for the minimum baseline for Collaboratory data, systems, activities and assets, but instead are intended in anticipation of increased security needs around specific projects, data, systems, activities and assets.

These policies do not and must not be interpreted to supersede any applicable law, higher level company directive, or existing labor-management agreement in effect as of the effective date of this policy.

While it may be applicable or even desirable in outside circumstances, this policy extends only as far as the authority of the Collaboratory and no further.

Policy Overview

In an effort to ensure an acceptable level of information security risk, Collaboratory is required to design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risk to its data and systems.

Collaboratory users are required to protect and ensure the Confidentiality, Integrity and Availability (CIA) of Collaboratory data and systems in accordance with the identified risk, regardless of how data is created, distributed or stored.

- Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and systems; and
- Security controls must be designed and maintained to ensure compliance with all applicable legal requirements.

Violations

Any Collaboratory user found to have violated any policy, standard, or procedure may be subject to disciplinary action, up to and including termination of access or Collaboratory employment. Damage caused by user violation of policy, standard or procedure may result in civil penalties as determined in a venue of appropriate jurisdiction. Violators of Federal, state, local, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Exceptions

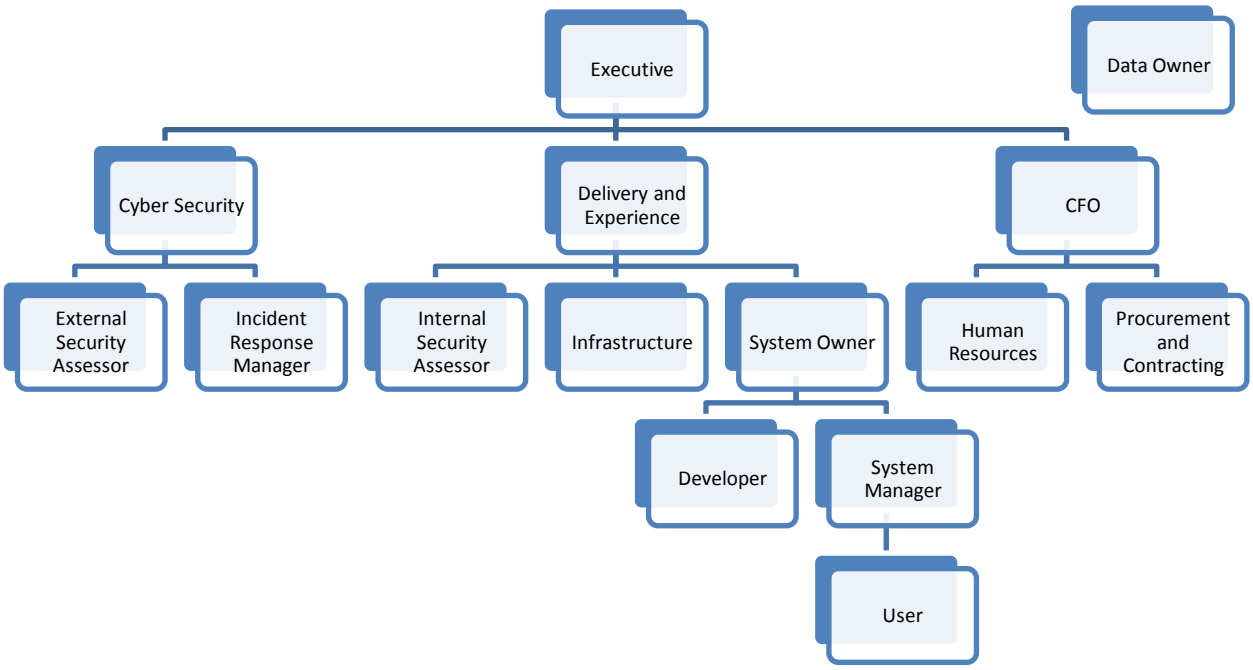
While any exception to a standard potentially weakens the protection mechanisms, occasionally exceptions will exist. Any exception to the policy and its associated procedures, standards and

guidelines must be documented by the party seeking an exception, then reviewed and recommended for approval by either the Vice President of Cyber Security or the Vice President of Delivery and Experience, and approved by an officer of the Collaboratory.

Updates

Updates to this policy or associated employees will be announced via management updates or email communication. Notifications of changes affecting only certain roles and responsibilities may be communicated in a matter that limits distribution only to those affected parties.

Roles and Responsibilities



Role Descriptions

Executive

Ultimate responsibility for security falls to the Executive (CEO/President). As such, all policies must be approved by the CEO prior to adoption.

Data Owner

A Data Owner is the individual (or organizational role) that provides data to the Collaboratory. Data Owners are empowered and responsible for communicating any distribution control requirements. A Data Owner is sometimes called an "Information Owner."

Cyber Security

Cyber Security drafts and recommends policies for acceptance by Delivery and Experience, performs incident response management, and provides external security assessment. Cyber Security also is mandated to provide counsel to system owners and the executive about the risk profile resultant of systems as implemented, to better inform the executive about organizational risk.

Incident Response Manager

Incident Response Managers provide a point of contact for security functions and coordinate intelligence gathering, security analysis, and response to real or perceived security incidents.

External Security Assessors

Truly external assessors, if required, will be under the mandate of the security function, and will necessarily fall outside the reporting chain of system owners, to ensure complete independence and impartiality.

Delivery and Experience

Delivery and Experience controls many operational and development functions. Delivery and Experience is accountable to the executive for risk decisions across all systems and services within his scope.

Infrastructure

Infrastructure is a special case of systems, which affect most if not all other systems. Infrastructure services standard IT functions (networking, printing, desktop, shared services, hardware provisioning, virtualization environments).

System Owner

System owners are responsible for an information system and the functions it provides to support the Collaboratory. System owners are empowered to make authorization decisions about resource allocation within an information system and to accept risks to a system.

System Manager

System managers are responsible for day-to-day maintenance, operations and support of one or more Collaboratory information system assets. Typically, system managers will be able to obtain enhanced access to systems to facilitate management, debugging, and maintenance.

Developer

Developers are responsible for the initial state of information systems, including authoring software and initial configurations, as well as providing updates to authored software to address functionality (faults, enhancements, and security issues).

Internal Security Assessor

Internal security assessors monitor the security of information systems and fall within the oversight of the system owner.

User

A user is someone who receives and relies upon services from an information system.

CFO (Administration)

Human Resources

The Human Resources role ensures that personnel are managed, trained, and accountable in the performance of their information security roles and responsibilities.

Procurement and Contracting

The financial function of management procurement provides oversight and accountability for decisions related to funds and resource allocations. In addition, it performs the role of ensuring that necessary security terms and conditions, including special security requirements, are part of relevant Collaboratory contracts and agreements.

Role Compatibility

The user role is compatible with all other roles.

External security assessors must not report to the system owner and must not be a system manager, internal security assessor, or system owner for any system they are an assessor to.

There is no inherent incompatibility between developers, internal security assessors, system managers, and even system owners. However, in multi-user environments, segmentation between these roles may be appropriate and desirable. The broader the criticality or impact of a system on the Collaboratory and its partners, the more important it is that system roles be separated.

There are no role compatibility issues with being a data owner.

Data Sources

Internally-Generated Information

Over the course of normal business activities, Collaboratory often generates new information, intellectual property, and the like. Whenever new information is generated, an internal Collaboratory Information Owner must be assigned for the new information. The manager of the business group generating the information is ordinarily designated as the Information Owner. The Information Owner must promptly report the existence of this new information for inclusion in the Collaboratory data dictionary. This new information must be labeled with the appropriate data classification category and treated appropriately.

Externally-Supplied Information

Over the course of normal business activities, Collaboratory often takes possession of third-party sensitive information. Whenever any information covered by a non-disclosure agreement has been acquired, an internal Collaboratory Information Owner must be assigned for information so received. The manager of the business group utilizing the information is ordinarily designated as the Information Owner. The Information Owner must promptly report the existence of this third-party information for inclusion in the Collaboratory data dictionary. This third-party information must be labeled with the appropriate data classification category and treated appropriately.

Data Classification

The Collaboratory will implement a simple four-mark classification system describing all information that the Collaboratory will generate, receive or otherwise come into contact with, as provided for in its Data classification policy.

Collaboratory will not access or possess data which it was not authorized to receive and will dispose of information based on its initial authorization to receive data. In cases where there is a subsequent binding modification to that authorization through license/contract adjustment or legal action, best reasonable effort will be used to implement any required changes in retention in a prompt manner.

For the purpose of this document, a Collaboratory Member is defined as one of: AEP, Battelle, Cardinal Health, Huntington, L Brands, Nationwide, or OhioHealth, and referred to “Collaboratory Members” or simply as “Members.”

Public

Information classified *Public* is not protected, and there is no reasonable expectation that Collaboratory will protect or in any way restrict access to Public information. Public information has no special restrictions about the systems on which it may be present or the transport mechanisms that may be used to transmit Public information.

Absent a specific classification, all Public Data is treated as:

SC {Public} = {(confidentiality, N/A), (integrity, N/A), (availability, N/A)}

Member Confidential, Sharable

Information classified *Member Confidential, Sharable* shall receive the level of protection described in this document but may be shared with and/or visible to any and all Collaboratory Members as long as the level of protection requirements are met.

Absent other classifications, Member Confidential, Sharable data is treated as:

SC {Member Confidential, Sharable} = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}.

(Member)Confidential, Restricted {Dissemination Control Tag}

Information classified *Confidential, Restricted* shall receive the level of protection described in this document and may not be shared with or visible to any party other than those listed in the Dissemination Control tag as long as the level of protection requirements are met.

Absent other classifications, Confidential Restricted data is treated as:

SC {Confidential, Restricted} = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}.

In cases where Confidential, Restricted data lists only Collaboratory Members, there is historical precedent to label the data as "Member Confidential, Restricted" rather than simply "Confidential, Restricted." Functionally, there is no difference in level of protection between "Member Confidential, Restricted" and "Confidential, Restricted" data and dissemination controls work in the same way.

Example: The label *Confidential, Restricted {AEP}* indicates protected information that is to be available only to the Collaboratory and AEP. All use, storage, and transmission of this protected information shall be compliant with the level of protection described in this document.

Example: The label *Member Confidential, Restricted {AEP, Nationwide, L Brands}* indicates protected information available only to the Collaboratory, AEP, Nationwide, and L Brands. All use, storage, and transmission of this protected information shall be compliant with the level of protection described in this document.

Example: The label *Confidential, Restricted {Widgets-R-Us}* indicates protected information available only to the Collaboratory and the fictitious non-Member client Widgets-R-Us, Inc. All use, storage, and transmission of this protected information shall be compliant with the level of protection described in this document.

Collaboratory Business Confidential

Information classified *Collaboratory Business Confidential* shall receive the level of protection described in this document and may not be shared with any party outside of the Collaboratory absent advance approval from a Collaboratory Officer. By default, all information will be treated as Collaboratory Business Confidential data unless and until otherwise classified.

Absent other classifications, Collaboratory Business Confidential data is treated as:

SC {Collaboratory Business Confidential} = {(confidentiality, Low), (integrity, Low), (availability, Low)}.

Information Security Control Objectives

Security control objectives are sometimes synonymous with standards. This policy's security control objectives have been organized to follow the structure of mandatory controls from NIST Special Publication 800-53 revision 4 to easily align and evaluate Collaboratory's security program to external security requirements. Furthermore, to facilitate audit and compliance work, each mandatory control is labelled with the NIST 800-53 revision 4 control identifier (in brackets). The Collaboratory security policy is intended to provide BASE (LOW) assurance on systems through mandatory controls. Additional controls, marked as [ENHANCED] are intended to be applied to enhance security to address specific requirements for Collaboratory assets, projects, data, systems, and activities.

Mandatory Base Level Controls

All Collaboratory systems are subject to the following baseline of common control objectives as described in this document, to provide assurance comparable to LOW assurance under NIST Special Publication 800-53 revision 4.

[AC-1] ACCESS CONTROL POLICY AND PROCEDURES
[AC-2] ACCOUNT MANAGEMENT
[AC-2 (4)] AUTOMATED AUDIT ACTIONS
[AC-3] ACCESS ENFORCEMENT
[AC-4] INFORMATION FLOW ENFORCEMENT
[AC-7] UNSUCCESSFUL LOGON ATTEMPTS
[AC-8] SYSTEM USE NOTIFICATION
[AC-14] PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
[AC-17] REMOTE ACCESS
[AC-17 (6)] PROTECTION OF INFORMATION
[AC-18] WIRELESS ACCESS
[AC-19] ACCESS CONTROL FOR MOBILE DEVICES
[AC-20] USE OF EXTERNAL INFORMATION SYSTEMS
[AC-20 (3)] NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES
[AC-22] PUBLICLY ACCESSIBLE CONTENT
[AT-1] SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
[AT-2] SECURITY AWARENESS TRAINING
[AT-3] ROLE-BASED SECURITY TRAINING
[AT-4] SECURITY TRAINING RECORDS
[AU-1] AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
[AU-3] CONTENT OF AUDIT RECORDS
[AU-4] AUDIT STORAGE CAPACITY
[AU-5] RESPONSE TO AUDIT PROCESSING FAILURES
[AU-6] AUDIT REVIEW, ANALYSIS, AND REPORTING
[AU-8] TIME STAMPS
[AU-9] PROTECTION OF AUDIT INFORMATION
[AU-11] AUDIT RECORD RETENTION
[AU-12] AUDIT GENERATION

[CA-1] SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
[CA-2] SECURITY ASSESSMENTS
[CA-2 (3)] EXTERNAL ORGANIZATIONS
[CA-3] SYSTEM INTERCONNECTIONS
[CA-5] PLAN OF ACTION AND MILESTONES
[CA-6] SECURITY AUTHORIZATION
[CA-7] CONTINUOUS MONITORING
[CA-7 (1)] INDEPENDENT ASSESSMENT
[CA-9] INTERNAL SYSTEM CONNECTIONS
[CM-1] CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
[CM-2] BASELINE CONFIGURATION
[CM-4] SECURITY IMPACT ANALYSIS
[CM-6] CONFIGURATION SETTINGS
[CM-7] LEAST FUNCTIONALITY
[CM-8] INFORMATION SYSTEM COMPONENT INVENTORY
[CM-10] SOFTWARE USAGE RESTRICTIONS
[CM-11] USER-INSTALLED SOFTWARE
[CP-1] CONTINGENCY PLANNING POLICY AND PROCEDURES
[CP-2] CONTINGENCY PLAN
[CP-3] CONTINGENCY TRAINING
[CP-4] CONTINGENCY PLAN TESTING
[CP-9] INFORMATION SYSTEM BACKUP
[CP-9 (1)] TESTING FOR RELIABILITY / INTEGRITY
[CP-10] INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
[IA-1] IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
[IA-2] IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
[IA-2 (1)] [IA-2 (2)] NETWORK ACCESS TO PRIVILEGED ACCOUNTS
[IA-2 (12)] ACCEPTANCE OF PIV CREDENTIALS
[IA-4] IDENTIFIER MANAGEMENT
[IA-5] AUTHENTICATOR MANAGEMENT
[IA-5 (1)] PASSWORD-BASED AUTHENTICATION
[IA-5 (11)] HARDWARE TOKEN-BASED AUTHENTICATION
[IA-6] AUTHENTICATOR FEEDBACK
[IA-7] CRYPTOGRAPHIC MODULE AUTHENTICATION
[IA-8] IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)
[IA-8 (2)] ACCEPTANCE OF THIRD-PARTY CREDENTIALS
[IA-10] ADAPTIVE IDENTIFICATION AND AUTHENTICATION
[IA-11] RE-AUTHENTICATION
[IR-1] INCIDENT RESPONSE POLICY AND PROCEDURES
[IR-2] INCIDENT RESPONSE TRAINING
[IR-3] INCIDENT RESPONSE TESTING
[IR-4] INCIDENT HANDLING
[IR-5] INCIDENT MONITORING
[IR-6] INCIDENT REPORTING
[IR-7] INCIDENT RESPONSE ASSISTANCE

[IR-8] INCIDENT RESPONSE PLAN
[MA-1] SYSTEM MAINTENANCE POLICY AND PROCEDURES
[MA-2] CONTROLLED MAINTENANCE
[MA-4] NONLOCAL MAINTENANCE
[MA-5] MAINTENANCE PERSONNEL
[MP-1] MEDIA PROTECTION POLICY AND PROCEDURES
[MP-2] MEDIA ACCESS
[MP-6] MEDIA SANITIZATION
[MP-7] MEDIA USE
[PE-1] PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
[PE-2] PHYSICAL ACCESS AUTHORIZATIONS
[PE-3] PHYSICAL ACCESS CONTROL
[PE-6] MONITORING PHYSICAL ACCESS
[PE-8] VISITOR ACCESS RECORDS
[PE-12] EMERGENCY LIGHTING
[PE-13] FIRE PROTECTION
[PE-14] TEMPERATURE AND HUMIDITY CONTROLS
[PE-15] WATER DAMAGE PROTECTION
[PE-16] DELIVERY AND REMOVAL
[PL-1] SECURITY PLANNING POLICY AND PROCEDURES
[PL-2] SYSTEM SECURITY PLAN
[PL-4] RULES OF BEHAVIOR
[PL-8] INFORMATION SECURITY ARCHITECTURE
[PS-1] PERSONNEL SECURITY POLICY AND PROCEDURES
[PS-2] POSITION RISK DESIGNATION
[PS-3] PERSONNEL SCREENING
[PS-4] PERSONNEL TERMINATION
[PS-5] PERSONNEL TRANSFER
[PS-6] ACCESS AGREEMENTS
[PS-7] THIRD-PARTY PERSONNEL SECURITY
[PS-8] PERSONNEL SANCTIONS
[RA-1] RISK ASSESSMENT POLICY AND PROCEDURES
[RA-2] SECURITY CATEGORIZATION
[RA-3] RISK ASSESSMENT
[RA-5] VULNERABILITY SCANNING
[SA-1] SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
[SA-2] ALLOCATION OF RESOURCES
[SA-3] SYSTEM DEVELOPMENT LIFE CYCLE
[SA-4] ACQUISITION PROCESS
[SA-4 (10)] USE OF APPROVED PIV PRODUCTS
[SA-5] INFORMATION SYSTEM DOCUMENTATION
[SA-9] EXTERNAL INFORMATION SYSTEM SERVICES
[SC-1] SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
[SC-5] DENIAL OF SERVICE PROTECTION
[SC-5 (1)] RESTRICT INTERNAL USERS

[SC-5 (2)] EXCESS CAPACITY / BANDWIDTH / REDUNDANCY
[SC-5 (3)] DETECTION / MONITORING
[SC-7] BOUNDARY PROTECTION
[SC-10] NETWORK DISCONNECT
[SC-12] CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
[SC-13] CRYPTOGRAPHIC PROTECTION
[SC-15] COLLABORATIVE COMPUTING DEVICES
[SC-20] SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
[SC-21] SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
[SC-22] ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
[SC-39] PROCESS ISOLATION
[SI-1] SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
[SI-2] FLAW REMEDIATION
[SI-3] MALICIOUS CODE PROTECTION
[SI-4] INFORMATION SYSTEM MONITORING
[SI-5] SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
[SI-12] INFORMATION HANDLING AND RETENTION

Enhanced Control Objectives

Additional controls may be applied to Collaboratory systems based on specific risk assessments and use cases. The following controls, in addition to the baseline described above, are intended to closely correspond to MODERATE assurance under NIST Special Publication 800-53 revision 4.

[ENHANCED] [AC-2 (1)] AUTOMATED SYSTEM ACCOUNT MANAGEMENT
[ENHANCED] [AC-2 (2)] REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS
[ENHANCED] [AC-2 (3)] DISABLE INACTIVE ACCOUNTS
[ENHANCED] [AC-5] SEPARATION OF DUTIES
[ENHANCED] [AC-6] LEAST PRIVILEGE
[ENHANCED] [AC-6 (1)] AUTHORIZE ACCESS TO SECURITY FUNCTIONS
[ENHANCED] [AC-6 (2)] NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS
[ENHANCED] [AC-6 (5)] PRIVILEGED ACCOUNTS
[ENHANCED] [AC-6 (9)] AUDITING USE OF PRIVILEGED FUNCTIONS
[ENHANCED] [AC-6 (10)] PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS
[ENHANCED] [AC-11] SESSION LOCK
[ENHANCED] [AC-11 (1)] PATTERN-HIDING DISPLAYS
[ENHANCED] [AC-12] SESSION TERMINATION
[ENHANCED] [AC-17 (1)] AUTOMATED MONITORING / CONTROL
[ENHANCED] [AC-17 (2)] PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION
[ENHANCED] [AC-17 (3)] MANAGED ACCESS CONTROL POINTS
[ENHANCED] [AC-17 (4)] PRIVILEGED COMMANDS / ACCESS
[ENHANCED] [AC-18 (1)] AUTHENTICATION AND ENCRYPTION
[ENHANCED] [AC-19 (5)] FULL DEVICE / CONTAINER-BASED ENCRYPTION
[ENHANCED] [AC-20 (1)] LIMITS ON AUTHORIZED USE
[ENHANCED] [AC-20 (2)] PORTABLE STORAGE DEVICES
[ENHANCED] [AC-21] INFORMATION SHARING
[ENHANCED] [AT-2 (2)] INSIDER THREAT
[ENHANCED] [AU-2] AUDIT EVENTS
[ENHANCED] [AU-2 (3)] REVIEWS AND UPDATES
[ENHANCED] [AU-3 (1)] ADDITIONAL AUDIT INFORMATION
[ENHANCED] [AU-6 (1)] PROCESS INTEGRATION
[ENHANCED] [AU-6 (3)] CORRELATE AUDIT REPOSITORIES
[ENHANCED] [AU-7] AUDIT REDUCTION AND REPORT GENERATION
[ENHANCED] [AU-7 (1)] AUTOMATIC PROCESSING
[ENHANCED] [AU-9 (4)] ACCESS BY SUBSET OF PRIVILEGED USERS
[ENHANCED] [CA-2 (1)] INDEPENDENT ASSESSORS
[ENHANCED] [CA-3 (5)] RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS
[ENHANCED] [CM-2 (1)] REVIEWS AND UPDATES
[ENHANCED] [CM-2 (3)] RETENTION OF PREVIOUS CONFIGURATIONS
[ENHANCED] [CM-2 (7)] CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS
[ENHANCED] [CM-3] CONFIGURATION CHANGE CONTROL
[ENHANCED] [CM-3 (2)] TEST / VALIDATE / DOCUMENT CHANGES
[ENHANCED] [CM-5] ACCESS RESTRICTIONS FOR CHANGE
[ENHANCED] [CM-7 (2)] PREVENT PROGRAM EXECUTION

[ENHANCED] [CM-7 (4)] UNAUTHORIZED SOFTWARE / BLACKLISTING
[ENHANCED] [CM-8 (1)] UPDATES DURING INSTALLATIONS / REMOVALS
[ENHANCED] [CM-8 (3)] AUTOMATED UNAUTHORIZED COMPONENT DETECTION
[ENHANCED] [CM-8 (5)] NO DUPLICATE ACCOUNTING OF COMPONENTS
[ENHANCED] [CM-9] CONFIGURATION MANAGEMENT PLAN
[ENHANCED] [CP-2 (1)] COORDINATE WITH RELATED PLANS
[ENHANCED] [CP-2 (3)] RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS
[ENHANCED] [CP-2 (8)] IDENTIFY CRITICAL ASSETS
[ENHANCED] [CP-4 (1)] COORDINATE WITH RELATED PLANS
[ENHANCED] [CP-6] ALTERNATE STORAGE SITE
[ENHANCED] [CP-6 (1)] SEPARATION FROM PRIMARY SITE
[ENHANCED] [CP-6 (3)] ACCESSIBILITY
[ENHANCED] [CP-7] ALTERNATE PROCESSING SITE
[ENHANCED] [CP-7 (1)] SEPARATION FROM PRIMARY SITE
[ENHANCED] [CP-7 (2)] ACCESSIBILITY
[ENHANCED] [CP-7 (3)] PRIORITY OF SERVICE
[ENHANCED] [CP-8] TELECOMMUNICATIONS SERVICES
[ENHANCED] [CP-8 (1)] PRIORITY OF SERVICE PROVISIONS
[ENHANCED] [CP-8 (2)] SINGLE POINTS OF FAILURE
[ENHANCED] [CP-10 (2)] TRANSACTION RECOVERY
[ENHANCED] [IA-2 (2)] NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS
[ENHANCED] [IA-2 (3)] LOCAL ACCESS TO PRIVILEGED ACCOUNTS
[ENHANCED] [IA-2 (8)] NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT
[ENHANCED] [IA-2 (11)] REMOTE ACCESS - SEPARATE DEVICE
[ENHANCED] [IA-3] DEVICE IDENTIFICATION AND AUTHENTICATION
[ENHANCED] [IA-5 (2)] PKI-BASED AUTHENTICATION
[ENHANCED] [IA-5 (3)] IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION
[ENHANCED] [IR-3 (2)] COORDINATION WITH RELATED PLANS
[ENHANCED] [IR-4 (1)] AUTOMATED INCIDENT HANDLING PROCESSES
[ENHANCED] [IR-6 (1)] AUTOMATED REPORTING
[ENHANCED] [IR-7 (1)] AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT
[ENHANCED] [MA-3] MAINTENANCE TOOLS
[ENHANCED] [MA-3 (1)] INSPECT TOOLS
[ENHANCED] [MA-3 (2)] INSPECT MEDIA
[ENHANCED] [MA-4 (2)] DOCUMENT NONLOCAL MAINTENANCE
[ENHANCED] [MA-6] TIMELY MAINTENANCE
[ENHANCED] [MP-3] MEDIA MARKING
[ENHANCED] [MP-4] MEDIA STORAGE
[ENHANCED] [MP-5] MEDIA TRANSPORT
[ENHANCED] [MP-5 (4)] CRYPTOGRAPHIC PROTECTION
[ENHANCED] [MP-7 (1)] PROHIBIT USE WITHOUT OWNER
[ENHANCED] [PE-4] ACCESS CONTROL FOR TRANSMISSION MEDIUM
[ENHANCED] [PE-5] ACCESS CONTROL FOR OUTPUT DEVICES
[ENHANCED] [PE-6 (1)] INTRUSION ALARMS / SURVEILLANCE EQUIPMENT
[ENHANCED] [PE-9] POWER EQUIPMENT AND CABLING

[ENHANCED] [PE-10] EMERGENCY SHUTOFF
[ENHANCED] [PE-11] EMERGENCY POWER
[ENHANCED] [PE-13 (3)] AUTOMATIC FIRE SUPPRESSION
[ENHANCED] [PE-17] ALTERNATE WORK SITE
[ENHANCED] [PL-2 (3)] PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES
[ENHANCED] [PL-4 (1)] SOCIAL MEDIA AND NETWORKING RESTRICTIONS
[ENHANCED] [RA-5 (1)] UPDATE TOOL CAPABILITY
[ENHANCED] [RA-5 (2)] UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED
[ENHANCED] [RA-5 (5)] PRIVILEGED ACCESS
[ENHANCED] [SA-4 (1)] FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
[ENHANCED] [SA-4 (2)] DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS
[ENHANCED] [SA-4 (9)] FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE
[ENHANCED] [SA-8] SECURITY ENGINEERING PRINCIPLES
[ENHANCED] [SA-9 (2)] IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES
[ENHANCED] [SA-10] DEVELOPER CONFIGURATION MANAGEMENT
[ENHANCED] [SA-11] DEVELOPER SECURITY TESTING AND EVALUATION
[ENHANCED] [SC-2] APPLICATION PARTITIONING
[ENHANCED] [SC-4] INFORMATION IN SHARED RESOURCES
[ENHANCED] [SC-7 (3)] ACCESS POINTS
[ENHANCED] [SC-7 (4)] EXTERNAL TELECOMMUNICATIONS SERVICES
[ENHANCED] [SC-7 (5)] DENY BY DEFAULT / ALLOW BY EXCEPTION
[ENHANCED] [SC-7 (7)] PREVENT SPLIT TUNNELING FOR REMOTE DEVICES
[ENHANCED] [SC-8] TRANSMISSION CONFIDENTIALITY AND INTEGRITY
[ENHANCED] [SC-8 (1)] CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION
[ENHANCED] [SC-17] PUBLIC KEY INFRASTRUCTURE CERTIFICATES
[ENHANCED] [SC-18] MOBILE CODE
[ENHANCED] [SC-19] VOICE OVER INTERNET PROTOCOL
[ENHANCED] [SC-23] SESSION AUTHENTICITY
[ENHANCED] [SC-28] PROTECTION OF INFORMATION AT REST
[ENHANCED] [SI-2 (2)] AUTOMATED FLAW REMEDIATION STATUS
[ENHANCED] [SI-3 (1)] CENTRAL MANAGEMENT
[ENHANCED] [SI-3 (2)] AUTOMATIC UPDATES
[ENHANCED] [SI-4 (2)] AUTOMATED TOOLS FOR REAL-TIME ANALYSIS
[ENHANCED] [SI-4 (4)] INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC
[ENHANCED] [SI-4 (5)] SYSTEM-GENERATED ALERTS
[ENHANCED] [SI-7] SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
[ENHANCED] [SI-7 (1)] INTEGRITY CHECKS
[ENHANCED] [SI-7 (2)] AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS
[ENHANCED] [SI-7 (7)] INTEGRATION OF DETECTION AND RESPONSE
[ENHANCED] [SI-8] SPAM PROTECTION
[ENHANCED] [SI-8 (1)] CENTRAL MANAGEMENT
[ENHANCED] [SI-8 (2)] AUTOMATIC UPDATES
[ENHANCED] [SI-10] INFORMATION INPUT VALIDATION
[ENHANCED] [SI-11] ERROR HANDLING
[ENHANCED] [SI-16] MEMORY PROTECTION

ACCESS CONTROL

[AC-1] ACCESS CONTROL POLICY AND PROCEDURES

a) All Collaboratory business systems must develop, adopt or adhere to a formal, documented access control procedure that addresses the purpose, scope, roles, responsibilities, management commitment, coordination between organization entities, and compliance.

Absent a specific document applying to a system or systems, all Collaboratory systems are to have restricted physical and logical access for Collaboratory personnel only, and only for the specific business purposes of that system.

b) All Access Control Policies and Procedures must undergo periodic review, such that
   1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.
   2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle

[AC-2] ACCOUNT MANAGEMENT

a) The Collaboratory maintains the following classes of accounts:

Guest User	Guest users do not require any form of authentication or specific authorization to obtain access to a limited set of Collaboratory resources. Guest users are, for example, the users of public websites or the remote senders of email to Collaboratory systems.
Individual User	This is the basic unit of account, which allows linkage of actions to a specific responsible party.
Emergency User	This is a temporary, emergency account which is created based on an acute business need without sufficient time to undergo normal authorizations. Issuing an emergency user account requires an account review within 30 days as described in AC-2(j) below.
Administrative User	Administrative users have the ability to change the class of account, the permissions associated with an account, and to modify the deployed behavior of a system that has users other than the administrative user.
Emergency Administrative User	This is a temporary, emergency account which is created based on an acute business need in an emergency situation without sufficient time to undergo normal authorizations. Such accounts should be issued only under circumstances where procedures must be suspended to respond to an emergency. Issuing an emergency administrative user account requires an account review within 30 days as described in AC-2(j) below.
System	Devices on Collaboratory networks.

Either class of emergency account should be documented and reviewed for lessons learned, and should prompt a full system review of privileges within 30 days as described in AC-2 (j) below.

Privileges, specific to the systems that accounts are created on, are assigned to accounts, to ensure appropriate use.

b) Every system under this policy will have an assigned system manager who is an employee or contractor within the Collaboratory. Should the system manager leave, the role of system manager will be assumed by the supervisor of that employee or contractor until management responsibility can be re-delegated to a new staff member or contractor.
c) Accounts will be assigned to groups (where a group is defined as accounts having a common set of system privileges) based on specific business needs. All systems will have a default group assignment for individual user accounts. Additional groups may be created based on a specific business reason (for instance, developers may need access to different resources, or specific employees may need access to sensitive data to perform their responsibilities). Any justification must be documented and the documentation and justification must be approved by the system manager.
d) Authorized users of systems must be documented, along with the business justification for the creation of their account.
e) System Managers must approve all account creations. System Managers may be directed to approve account creations by their supervisors or management.
f) System Managers must develop or adopt documented procedures for account creation, modification, disabling or removal for their systems. Absent a system-specific document:
    - Accounts will be created only when directed by management and under specified conditions under which the account will be active (for example, a period of time);
    - Accounts will be modified when directed by management or when the specified conditions for the account's creation have changed; or if technical conditions require a change to the account to continue authorized functionality;
    - Accounts will be disabled upon termination of association with the Collaboratory or when the conditions that justify the creation of the account no longer exist;
    - Accounts will be removed only after being disabled and a determination that the account will no longer be needed has been made by the creating authority or the business records retention period has elapsed since account disabling.
g) System accounts, privileges, and use will be periodically monitored to ensure that current accounts and authorizations are consistent with business needs;
h) Systems managers will notify the authorizing authority of the account within 30 days of a change that:
    - An account is no longer required;
    - When users are terminated or transferred; or
    - Whenever information system uses or need-to-know changes.

i) Authorization to Collaboratory information systems will be granted based on:
   - Valid access authorizations;
   - Intended system usage; and
   - Any other attributes as required by the Collaboratory to achieve specific business functions, as documented in a system-specific document.

j) Account information will be reviewed by the system manager at least once per fiscal year, with communication to the authorizing authorities and the System Owner or his/her designee (by email or in writing) of any divergences from organization requirements. This review must also occur no more than 30 days after the issuance of an emergency individual user or emergency administrative account.

k) Whenever shared credentials are deployed, procedures will be established to re-issue those credentials when any individual having access is no longer authorized.

[ENHANCED] [AC-2 (1)] AUTOMATED SYSTEM ACCOUNT MANAGEMENT

The organization will employ automated mechanisms to support the management of information system accounts to the extent supported by the operating systems and devices in use.

[ENHANCED] [AC-2 (2)] REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS

Emergency individual accounts must be suspended after 1 business day, be re-authorized for an additional day, or be converted to a normal individual account through the normal authorization process.

Emergency administrative accounts must be suspended or re-authorized after 1 business day, or the emergency ends, whichever comes first.

No emergency account should be active without an initial/re-authorization having occurred no earlier than the previous business day.

[ENHANCED] [AC-2 (3)] DISABLE INACTIVE ACCOUNTS

Inactive accounts will be disabled or suspended after a period of 21 days.

[AC-2 (4)] AUTOMATED AUDIT ACTIONS

All systems will be configured to automatically audit the account creation, modification, enabling, disabling, and removal actions. Audit results will be sent to the system manager.

[AC-3] ACCESS ENFORCEMENT

The information system will enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies as designed into applications, operating systems and network segmentation/firewall rules.

[AC-4] INFORMATION FLOW ENFORCEMENT

The organization will maintain current documentation of network firewall behaviors and will maintain a firewall sufficient to segment systems and data from improper data flows.

[ENHANCED] [AC-5] SEPARATION OF DUTIES

Responsibilities will be segmented across multiple individuals (to the extent possible within the organizational structure) to limit the potential for abuse or malevolent activity without requiring collusion. All segmentation of duties will be documented and implemented through access authorizations.

[ENHANCED] [AC-6] LEAST PRIVILEGE

All Collaboratory systems must employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

[ENHANCED] [AC-6 (1)] AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Security functions are only to be performed by explicitly authorized individuals, with authorization being granted by the System Owner. All individuals authorized to perform security functions will be listed in a paper document (official) with an electronic backup (draft) in the custody of the System Owner.

Security functions minimally include:

- Establishment of system accounts
- Configuration of access authorizations (permissions, privileges)
- Configuration of audit and logging functions
- Configuration of intrusion detection parameters
- Configuration of routing and firewall filtering rules
- Cryptographic key management functions for systems or groups of users
- Security service configuration
- Access control list configuration

Additional security functions may be noted on a system-by-system basis.

[ENHANCED] [AC-6 (2)] NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

Any user authorized to perform or having access to security functions will use non-privileged accounts or functional roles when accessing non-security functions.

[ENHANCED] [AC-6 (5)] PRIVILEGED ACCOUNTS

Privileged accounts will be issued only to employees and contractors of the Collaboratory needing those privileges.

[ENHANCED] [AC-6 (9)] AUDITING USE OF PRIVILEGED FUNCTIONS

Any execution of system privileged functions will be audited.

[ENHANCED] [AC-6 (10)] PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Collaboratory information system will prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

[AC-7] UNSUCCESSFUL LOGON ATTEMPTS

Collaboratory information systems will automatically perform the following handling of unsuccessful or invalid login attempts:

a) Systems will respond to consecutive login attempts by a user during a fixed period by locking the account for a pre-defined period of time. This must be configured and documented on a per-system basis. Absent other guidance, systems will react to consecutive login attempt failures with an increasing delay for the next login prompt, ten seconds per consecutive failure.
b) All such failure attempts must generate a logging trail of the failed login attempts, and do at least one of the following
    - Lock the account/node until released by a system manager
    - Lock the account/node for a period of time appropriate to the impact of the system
    - Delay next login prompt for a period of time appropriate to the impact of the system

[AC-8] SYSTEM USE NOTIFICATION

Human interfaces (such as workstation terminals and remote login protocols) will use notification mechanisms to provide constructive privacy and security notices consistent with all applicable Federal, state, local and contractual legal requirements. All system use notification messages (“banners”) will:

a) Be prominently displayed at human interfaces for all Collaboratory systems prior to granting access.
b) Specify that information system usage may be monitored, recorded, and is subject to audit and review;
c) Specify that unauthorized use of the information system is prohibited and is subject to criminal and civil penalties;
d) Specify that use of the information system indicates consent to monitoring and recording;
e) Require that an act of acknowledgement (click through or other explicit action) occur prior to the banner leaving the screen and prior to login authorization occurring.

[ENHANCED] [AC-11] SESSION LOCK

User consoles will implement a temporary locking mechanism so that users can stop working and move away from the immediate vicinity for temporary interruptions.

a) Session locks will automatically occur after no more than 3 minutes of inactivity, or upon user request.
b) Session locks will persist until the user re-establishes access using established identification and authentication processes.

[ENHANCED] [AC-11 (1)] PATTERN-HIDING DISPLAYS

Session locks will conceal any information previously visible on the display with a public-grade image (screensaver).

[ENHANCED] [AC-12] SESSION TERMINATION

Remote access services will be configured to terminate sessions after 3 hours of inactivity.

[AC-14] PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Absent specific and compelling business reasons to the contrary, Collaboratory systems will disable guest user access. Any guest user access system must have a document on file which:

a) Identifies permitted actions available to guest users on the Collaboratory system.
b) Describes the supporting rationale for permitting those actions to guest users.

[AC-17] REMOTE ACCESS

Remote access (access from any physical location or network outside of approved facilities) to Collaboratory resources is not permitted except in those cases which are documented and authorized as described below.

Exceptions	Access restrictions
Public website and documents Domain Name System public records Sending email to Columbus Collaboratory users	PUBLIC - no general restrictions on remote access; rate limitations and responses to real or perceived abusive behavior may restrict specific access.
Email retrieval for Columbus Collaboratory email domain users.	Only on approved devices with configurations conforming to this security policy

a) Usage restrictions, configuration and connection requirements, and implementation guidance for each type of remote access must be documented and met.
b) Remote access must be authorized (approved) at the Vice President level or above, or part of a blanket authorization included in this policy.

[ENHANCED] [AC-17 (1)] AUTOMATED MONITORING / CONTROL

Any information system that provides remote access services must also have monitoring of and control of remote access methods.

[ENHANCED] [AC-17 (2)] PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION

Remote access communication for any non-public information must be use appropriate encryption for the risk and impact of the data and system being accessed.

[ENHANCED] [AC-17 (3)] MANAGED ACCESS CONTROL POINTS

All remote access must be routed through the network firewall and its upstream network connections.

[ENHANCED] [AC-17 (4)] PRIVILEGED COMMANDS / ACCESS

a) The use of privileged commands and access to security-relevant information via remote access is prohibited, except when
b) The rationale for such access has been documented and approved at the Vice President level or higher.

[AC-17 (6)] PROTECTION OF INFORMATION

Users are required to protect information about any authenticated remote access mechanism from unauthorized use and disclosure, including but not limited to any network addresses, authentication credentials, and usage procedures involved.

[AC-18] WIRELESS ACCESS

a) Collaboratory will establish configuration guidelines, usage restrictions and implementation guidance for wireless access; and
b) Any wireless access to information systems will be authorized prior to permitting such connections. Because of the reliance on wireless infrastructure within the Collaboratory for end-user stations; wireless interfaces for Collaboratory personnel will be authorized as part of the deployment process by the System Manager.

[ENHANCED] [AC-18 (1)] AUTHENTICATION AND ENCRYPTION

Collaboratory will permit only wireless access to Collaboratory systems which use authentication of users or devices, and an encryption method appropriate to and commensurate with the risk associated with any Collaboratory system the wireless-connected systems can access.

[AC-19] ACCESS CONTROL FOR MOBILE DEVICES

A mobile device, for purposes of this policy, is any device which can either collect or output information; with a form factor that can be easily carried by a single individual, is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source.

a) Collaboratory will establish configuration guidelines, usage restrictions and implementation guidance for organization-controlled mobile devices; and
b) Any mobile device access to information systems will be authorized prior to permitting such connection.

[ENHANCED] [AC-19 (5)] FULL DEVICE / CONTAINER-BASED ENCRYPTION

All organization-owned mobile devices will utilize either container-based encryption (on any container accessing any Collaborator data or system which is not public) or full-device encryption (if container-based encryption is either unavailable or undesirable).

[AC-20] USE OF EXTERNAL INFORMATION SYSTEMS

All external information systems utilized by the Collaboratory to access non-public Collaboratory data will be governed by terms of use consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a) access the information system from external information systems; and
b) Process, store, or transmit organization-controlled information using external information systems.

[ENHANCED] [AC-20 (1)] LIMITS ON AUTHORIZED USE

Authorized individuals may use an external information system to access the information system or to process, store, or transmit Collaboratory information only when the organization:

a) Verifies the implementation of required security controls on the external system as specified in the Collaboratory's information security policy; or
b) Retains approved information system connection or processing agreements with the external information system's operating entity.

[ENHANCED] [AC-20 (2)] PORTABLE STORAGE DEVICES

The use of Collaboratory-controlled portable storage devices by authorized individuals on external information systems is prohibited. Exceptions to this prohibition may be granted at the system manager or above level only when sufficient security measures, commensurate with the associated risk, are put into place to prevent the infiltration of malicious data or exfiltration of non-public data.

[AC-20 (3)] NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES

The use of devices not owned or (contractually) controlled by the Collaboratory to interact with non-public Collaboratory systems and data is prohibited. Exceptions to this prohibition may be granted at the system manager or above level only when sufficient security controls are implemented in the non-organizationally owned system. Exceptions will be limited to specific information, services and applications and will be governed by written Collaboratory approved terms of use prior to being granted.

[ENHANCED] [AC-21] INFORMATION SHARING

Labelling and procedures described in the information and information systems classification policy will be followed, which is provided in summary table below.

Data Type	AC-21a: Discretionary disclosure criteria	AC-21b: Decision facilitation mechanisms
Public	Full discretion	• Labelling of data/data container
Member Confidential, Sharable	Disclosure to Collaboratory members meeting protection requirements of data.	• Labelling of data or containers with data;

		• Verification of identification of recipient based on existing Collaboratory relationships • Requires assertion by recipient of data protection requirements being met.
Member Confidential, Restricted	Disclosure to Collaboratory member organizations or individuals meeting protection requirements of data.	• Labelling of data or containers with data; • Verification of identification of recipient based on existing Collaboratory relationships • Requires assertion by recipient of data protection requirements being met.
Collaboratory Business Confidential	Disclosure only with approval by a Collaboratory Officer	

[AC-22] PUBLICLY ACCESSIBLE CONTENT

For all publicly accessible content, the Collaboratory will:

a) Designate individuals authorized to post information onto publicly accessible information systems;
b) Train authorized individuals to ensure that publicly accessible information does not contain non-public information;
c) Review proposed content of information prior to posting onto publicly accessible information systems to ensure that nonpublic information is not included;
d) Review the content of publicly accessible information systems to ensure that no non-public information whenever changes are made and no less frequently than once every fiscal year. Should non-public information be discovered, it will be removed from public information systems as quickly as possible.

AWARENESS AND TRAINING

[AT-1] SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

a) The Collaboratory will develop security training for appropriate audiences.
    1. Security training will, at a minimum, cover the following topics:
        - The individuals' role in Collaboratory security
        - Appropriate procedures and processes governing that individual's role
        - The mandatory security controls affecting that individual's roles.
        - The appropriate escalation path to raise security concerns and issues
        - The purpose and scope of Collaboratory's security policies and procedures
        - Management commitment to Collaboratory security
        - Roles and responsibilities for security
        - Coordination within and without the Collaboratory of security efforts
        - Security Compliance at the Collaboratory
        - Recognizing and reporting potential indicators of insider threats (see AT-2(2) below).
    2. Mechanisms, approved by senior management, will be established for managing initial and recurring training, and appropriate mechanisms for training will be approved by management. Absent other guidance:
        - Copies of the relevant security policies will be provided;
        - Questions about the applicability of the policy will be answered by a knowledgeable Collaboratory-approved individual, with questions being captured in writing so that frequently asked questions and training materials can be improved over time;
        - Confirmation that the policy has been read and understood by each affected individual will be provided, in writing.

b) All Access Control Policies and Procedures must undergo periodic review, such that
    1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.
    2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle.

[AT-2] SECURITY AWARENESS TRAINING

All system users—including but not limited to managers, senior executives, and contractors—will receive basic security awareness training about Collaboratory systems and security.

a) As part of initial training for new users;
b) When required by information system changes;
c) Re-training of all relevant security training material will be required to occur at least once every 18 months, with a preferred cycle of once every 12 months.

[ENHANCED] [AT-2 (2)] INSIDER THREAT

Security awareness programs must include training on recognizing and reporting potential indicators of insider threats. Examples of potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of organizational policies, procedures, directives, rules, or practices.

The awareness program will articulate approved methods to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.

[AT-3] ROLE-BASED SECURITY TRAINING

Extended security training, beyond minimal policy awareness, will also be provided based on the security roles and responsibilities that individuals fulfill within the Collaboratory. Said training is mandatory and will be completed:

a) Prior to authorizing access to information systems or performing assigned security responsibilities;
b) When required by information system changes; and
c) Re-training of all relevant security training material will be required to occur at least once every 18 months, with a preferred cycle of once every 12 months.

[AT-4] SECURITY TRAINING RECORDS

Security training records will be maintained in a central (paper) repository and reviewed no less than once every 12 months.

a) Records will document individual information system training activities including basic security awareness training and specific information system security training.
b) Individual training records will be maintained for a minimum of 4 years.

AUDIT AND ACCOUNTABILITY

[AU-1] AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

a) Any non-public system, or system that processes non-public information, will at a minimum generate auditable event (observable occurrence) activity log as required to comply with all applicable Federal, state, local and contractual legal requirements. Systems which are unable to support this requirement can be exempted if their existence is documented and approved within the risk management guidelines of the Collaboratory, but any system incapable of supporting the audit requirements must not be used for information processing any non-public information.

   Barring stronger, system-specific documentation, the auditable trail will be reviewed by automation or manually by system staff if automation is not available for violations and fault identification. Audit trails must be retained for a minimum of 28 days.

   1. This policy will be reflected in the mandatory, approved login banners (see Access Control section AC-8) to ensure constructive notification and included in the Collaboratory's security awareness training regimen.
   2. The Collaboratory will document any necessary procedures to facilitate this audit and accountability policies must be documented.

b) All Audit and Accountability Policies and Procedures must undergo periodic review, such that
   1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.
   2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle

[ENHANCED] [AU-2] AUDIT EVENTS

Prior to deployment, any system required to generate audit and accountability records must be determined to be capable of doing so and procedures must exist to audit those events, if they are required (even if there is no requirement to actually performing such audits).

a) The following security events must be auditable on any system having non-public information or any non-public system: successful login; password changes; failed logins; failed accesses to information systems; administrative privilege usage; personal identity verification credential usage; third-party credential usage; account creation; assignment or changes to system privileges or group memberships.
b) Audit information will be made available on a business requirement basis to any part of the Collaboratory requiring that access, as approved by executive management.

c) The necessary records will be sufficient to construct a trail of which party was authorized to perform various actions, based on essential tracking user behavior and privilege behavior to establish means and opportunity for an account to have been used in an event.

[ENHANCED] [AU-2 (3)] REVIEWS AND UPDATES

Section AU-2 will be reviewed no less frequently than once every 39 months (3 years, 3 months) with a preferred 3-year cycle, or as involved underlying technologies undergo substantive changes.

[AU-3] CONTENT OF AUDIT RECORDS

All Collaboratory audit records must contain information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

[ENHANCED] [AU-3 (1)] ADDITIONAL AUDIT INFORMATION

Audit records must not contain any information that internal or external auditors would not be permitted to have access to under Federal, state, local, or contractual legal requirements. Any audit record types requiring more detailed information must be documented and appropriately classified prior to deployment.

[AU-4] AUDIT STORAGE CAPACITY

Sufficient space will be allocated to store a minimum of at least twice the expected audit data as required by this policy.

[AU-5] RESPONSE TO AUDIT PROCESSING FAILURES

In the event of an automated audit processing failure, information systems will fail as safely as possible.

a) Generate an error message for the system manager that the audit processing failure occurred. Such error messages must be transmitted to the system manager either through system-specific procedures or via established protocols (electronic mail).
b) Following an audit processing failure, the system may overwrite the oldest stored audit record and, if that also fails or is not attempted, shut down the system.

[AU-6] AUDIT REVIEW, ANALYSIS, AND REPORTING

Human analyst review is required for all systems. Automated analysis of audit data will be implemented and used to identify inappropriate or unusual activity over time, to facilitate technical fault identification and resolution, identify misuse and violations of system policies, and to inform resource requirements and security requirements.

a) For systems having automated analysis in place, manual reviews must occur before log data retention forces the removal of the audit logs; for systems not having automated analysis in place, manual reviews must occur before log data retention forces the removal of the audit logs and no less frequently than once per week.

b) Reports of all audit findings will be made to the System Manager, and escalated into management when problems are strongly suspected or identified.

[ENHANCED] [AU-6 (1)] PROCESS INTEGRATION

The Collaboratory will employ automated mechanisms to integrate audit review, analysis, and reporting processes. Absent system-specific documentation to the contrary, automation is expected to be implemented, tested and deployed for all systems within one year of implementation.

[ENHANCED] [AU-6 (3)] CORRELATE AUDIT REPOSITORIES

Barring system-specific documentation with a clear business case to the contrary, all audit records will be transferred to a central audit record management system and all systems sending audit records will have synchronized time as required in AU-8 below.

[ENHANCED] [AU-7] AUDIT REDUCTION AND REPORT GENERATION

The central audit record management system will provide for the reduction of audit data into generated reports which:

a) Support on-demand audit review, analysis and reporting requirements (should they exist) and after-the-fact investigations of suspicious incidents;
b) The central audit record management system will not alter the original content or time stamp ordering of audit records. No part of this policy should be interpreted to require that all reports be ordered by timestamp, but being able to correlate the original timestamp-ordered events is a fundamental requirement of central audit record management.

[ENHANCED] [AU-7 (1)] AUTOMATIC PROCESSING

The audit log processor will, at a minimum, provide the capability to process audit records for events of interest based on what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

[AU-8] TIME STAMPS

Audit logs from information will be timestamped and will be kept in Universal Coordinated Time (UTC) (absent documented technical barriers to implementation). Most modern computing devices are implemented with logging precision within 1 second; however, all timestamps:

a) Will be generated using the internal system clock of the system generating the audit log;
b) Will be accurate based on the following chart:

System Type	Minimum level of precision required
Networking infrastructure (for example, firewalls, switches, access points and routers)	Within 1 second
Servers	Within 2 seconds
Any other type of device	Within 60 seconds

[ENHANCED] [AU-8 (1)] SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

Information systems will compare internal system clocks to an authoritative time source and synchronize to maximize timestamp accuracy. System-specific guidance overriding this policy will only be approved to generate a more accurate timestamp mechanism or address timestamp management deficiencies on specific system platforms.

Barring system-specific guidance to the contrary:

a) Systems will rely on high-accuracy network time sources operated by the Collaboratory, or provided by trusted vendors such as NIST, Microsoft, and Apple, with a check occurring from each system at least once every 6 hours.
b) Systems will use a (simple) Network Time Protocol service implementation to force clock convergence.

[AU-9] PROTECTION OF AUDIT INFORMATION

Systems will protect all audit information and tools from unauthorized access, modification and deletion.

[ENHANCED] [AU-9 (4)] ACCESS BY SUBSET OF PRIVILEGED USERS

Only system managers are authorized to modify audit functionality.

[AU-11] AUDIT RECORD RETENTION

Audit records are retained for a minimum of 28 days; system-specific documentation may mandate longer periods or, in the absence of technical support for 28 days of audit record retention, as long as the system can be configured to retain such records.

[AU-12] AUDIT GENERATION

a) A summary of audit log generation will be drafted by the system manager of each information system and integrated and kept on file.
b) System managers are responsible for ensuring that system configurations support the audit requirements; software developers are responsible for ensuring that such audit requirements can be implemented; procurement is responsible for ensuring that systems purchased have the necessary capabilities to ensure auditability.
c) System managers are responsible for documenting that each of their systems can in fact comply with AU-2 and AU-3 requirements above.

SECURITY ASSESSMENT AND AUTHORIZATION

[CA-1] SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Security assessment and authorization occurs to: ensure that information security is built into Collaboratory information systems; identify weaknesses and deficiencies early in the development process; inform risk-based decisions as part of the security authorization process; and ensure compliance to vulnerability policies and procedures.

System security assessment will occur at least once every 15 months, with a preferred 1-year cadence, unless described in system-specific documentation on a more frequent basis. Security assessments will also occur on an as-needed basis in light of changes to technology or discovery of vulnerabilities, as required, to remediate specific system and information risk.

System-specific assessment methodology and procedures will be documented and defined at the time that systems are deployed and will be reviewed and revised at least once every 39 months with a preferred 3-year cadence unless described in system-specific documentation as being required on a more frequent basis. Evaluation of the need to revise (and appropriate revisions, if required) should also be prompted when new vulnerabilities become known affecting deployed systems.

[CA-2] SECURITY ASSESSMENTS

In the absence of specific procedures, security assessment will require a complete software and system inventory, a full review of known vulnerabilities for those systems and software, network and device connectivity audits with physical touch of any asset required, full network and system vulnerability scans targeted to those specific systems and software, review of all settings and configurations, review of all accounts and account authorizations on systems being mapped directly to written authorization records, audit of all security event records, review of past security incidents, review of all firewall configurations, and complete review of all personnel changes (adding or terminating personnel or any change in roles/responsibilities) occurring since the previous review.

The Collaboratory will:

a) Generate a specific schedule and plan for the security review of each information system that identifies:
    1. Specific controls and control enhancements to be assessed;
    2. Procedures and methods used to evaluate those controls and enhancements;
    3. Specify the evaluation personnel, environment, roles and responsibilities within the evaluation model.
b) Make a determination within the evaluation environment as to whether the controls in the information system(s) are operating as intended, as well as the extent to which the controls are implemented correctly and producing the desired outcome with respect to meeting established security requirements;
c) Produce a security assessment report that documents the results of the assessment; and

d) Provides the results of the security control report to the System Owner and, if accepted, to Security and the Executive.

[ENHANCED] [CA-2 (1)] INDEPENDENT ASSESSORS

Security assessors and assessment teams must be technically knowledgeable, sufficiently qualified and impartial to make a fair and honest assessment. To facilitate this, no system manager may provide the assessment of security adequacy of a system s/he directly manages. System managers will cooperate with the security assessor to the extent necessary to provide a meaningful assessment. If an internal System Owner resource that is impartial, technically knowledgeable and sufficiently qualified is unavailable, the Collaboratory will, through the Security group, obtain an external security assessor.

[CA-2 (3)] EXTERNAL ORGANIZATIONS

The Collaboratory will accept the assessment of external evaluators only when the assessment scope is documented to meet or exceed the minimum internal requirements for security assessment and is performed by an appropriately vetted and contracted third party.

[CA-3] SYSTEM INTERCONNECTIONS

System interconnections refer to persistent technical interfaces provided across security boundaries such as firewall zones or administrative control boundaries where one end is not controlled by the Collaboratory.

a) Every system interconnection will be documented and agreed to in writing by authorizing parties on both sides of the interconnection.
b) Each system interconnection agreement will document the interface characteristics, security requirements, and nature of the information communicated. Collaboratory will generate an internal risk profile for the system interconnection identifying associated technical and organizational risks and accept the risk (as mitigated by implementation of the security requirements) prior to authorizing the interconnection.
c) All system interconnection agreements will be reviewed at least once every 15 months, with a preferred cadence of annually; or more frequently if circumstances (interface characteristics, security requirements, nature of information, or risk profile) should change.

[ENHANCED] [CA-3 (5)] RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

The Collaboratory will, by default, deny all interconnections with external systems. Permission for interconnection will be granted on a case-by-case basis.

[CA-5] PLAN OF ACTION AND MILESTONES

The Collaboratory will document:

a) A plan of action and milestones for each information system to document discovery, intended remediation, and completion of remedial actions to correct weaknesses or deficiencies noted during security assessment of the security controls, to reduce or eliminate known vulnerabilities

in Collaboratory systems. System Managers are responsible for generating, tracking, and reporting on the plan for their systems; System Owner is responsible for collating a comprehensive plan.

b) The plan of action will be updated at least quarterly to demonstrate planned, progressing, stalled, or abandoned efforts.

[CA-6] SECURITY AUTHORIZATION

Decisions to authorize an information system will occur by the System Owner.

a) Authorizations will come from an individual who is supervisory to the affected system manager.
b) Authorization will occur prior to an information system processing information in a non-testing/development manner
c) Authorizations will be reviewed and updated at least once per fiscal year.

[CA-7] CONTINUOUS MONITORING

Collaboratory System Managers and Security will remain current with respect to knowledge of security vulnerabilities, threats, and current security techniques and tools. Affected personnel will monitor security vulnerability and patch information from trusted sources, including but not limited to affected vendors and US-CERT.

The Collaboratory will develop a comprehensive strategy to implement continuous monitoring which:

a) Establishes metrics to be monitored;
b) Establishes a frequency of monitoring and frequency for assessments supporting of monitoring;
c) Performs ongoing security control assessments;
d) Monitors security status of the organization's defined metrics;
e) Correlates and analyzes security-related information generated by assessment and monitoring;
f) Specifies response actions to address the results of the analysis of security-related information;
g) Reports security status of the Collaboratory to System Owner, Security, and the Executive on a schedule no less frequently than annually;

[CA-7 (1)] INDEPENDENT ASSESSMENT

Collaboratory's security controls will be subject to continuous assessment performed by independent assessors, providing for fair, honest and impartial assessment. To meet this requirement, assessors must not:

- Create a mutual or conflicting interest with the organizations where the assessments are being conducted;
- Assess their own work;
- Act as management or employees of the organizations they are serving; or
- Place themselves in advocacy positions for the organizations acquiring their services.

[CA-9] INTERNAL SYSTEM CONNECTIONS

An internal system interconnection refers to persistent technical interfaces provided across security boundaries such as firewall zones or administrative control boundaries where both sides are controlled by the Collaboratory.

a) Every internal system interconnection will be documented and authorized by appropriate Collaboratory personnel. Internal system interconnections may be authorized for groups or classes of equipment, rather than by individual systems (e.g. “all workstations on the Collaboratory LAN may print to the main printer”).
b) Internal system interconnections will have documented the interface characteristics, security requirements, and nature of the information communicated. Collaboratory will generate an internal risk profile for the system interconnection identifying associated technical and organizational risks and accept the risk (as mitigated by implementation of the security requirements) prior to authorizing the interconnection.
c) All system interconnection agreements will be reviewed as needed when circumstances (interface characteristics, security requirements, nature of information, or risk profile) change.

CONFIGURATION MANAGEMENT

[CM-1] CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Collaboratory will follow system-specific procedures and guidelines for configuration management.

a) System Managers are responsible for following configuration guidelines and procedures. Configuration guidelines may be drafted by developers or system managers, but must undergo an independent review prior to approval, to ensure appropriate protections are in place to meet organizational objectives.
b) Mandatory reviews:
    1. This policy will undergo review at least once every 39 months, with an intended cadence of once every 3 years. This policy must be reviewed following any security incident.
    2. All configuration guidelines must be reviewed at least once every 15 months, with an intended cadence of once every year. In addition, configuration guidelines must be reviewed following the discovery of vulnerabilities in software or systems or following any security incident.

[CM-2] BASELINE CONFIGURATION

Collaboratory will document baseline configurations for classes of information systems, with specific information system requirements documented as exceptions or additions. Each document will retain that configuration under change control, and maintain a backup of configuration parameters so that a system can be returned to baseline when needed.

[ENHANCED] [CM-2 (1)] REVIEWS AND UPDATES

Collaboratory will review and update baseline configurations of information systems:

a) At least once every 15 months, with a preferred cadence of annually;
b) When required to respond to changes in technology, risk profile, vulnerability discovery, or in response to a security incident; and
c) As an integral part of information system component installations and upgrades.

[ENHANCED] [CM-2 (3)] RETENTION OF PREVIOUS CONFIGURATIONS

Collaboratory will retain at a minimum the previous working configuration to support rollback.

[ENHANCED] [CM-2 (7)] CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

Normal Collaboratory information systems are not permitted to be transferred into areas deemed “high-risk” by the Collaboratory. Should a Collaboratory staff member need to travel to those high-risk areas and should the organization determine that the risk of the individual not having access to equipment is unacceptable to the organization:

a) Appropriate minimal device support will be provided that has been sanitized of sensitive data and configured to meet only those requirements of the travel;
b) Any such device will be sanitized (at a minimum, a low-level format and re-imaged to a baseline level) and then will be permanently labelled to prevent access to any non-public data in the future.

[ENHANCED] [CM-3] CONFIGURATION CHANGE CONTROL

For each class of information system, or describe in terms of divergence from standard class for an individual information system, Collaboratory will:

a) Determine the type of changes to information systems that are configuration-controlled;
b) Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analysis;
c) Document configuration change decisions associated with the information system;
d) Implement approved configuration-controlled changes to the information system;
e) Retain records of all configuration controlled changes for a minimum period, which must be at least the shorter of 3 years or 1 year following the retirement and decommissioning of an information system;
f) Audit and review activities associated with configuration-controlled changes to the information system;
g) Coordinate and review configuration change control activities with all system managers and a representative of Security at least once per quarter.

[ENHANCED] [CM-3 (2)] TEST / VALIDATE / DOCUMENT CHANGES

Collaboratory will test, validate and document any and all changes to an information system prior to implementing the changes on the operational system.

[CM-4] SECURITY IMPACT ANALYSIS

Collaboratory will analyze changes to the information system to determine potential security impacts prior to change implementation.

[ENHANCED] [CM-5] ACCESS RESTRICTIONS FOR CHANGE

The Collaboratory will define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

[CM-6] CONFIGURATION SETTINGS

The Collaboratory will establish and document configuration settings for information technology products employed within the information system.

a) Configuration settings will be consistent with operating system and application security configuration checklists published by NIST or the Center for Internet Security, reflecting the most restrictive mode consistent with operational requirements.

b) Configuration settings will be implemented as documented.
c) Documentation will reflect identification and approval of any deviation from established configuration settings for any Collaboratory components based on documented and approved operational requirements.
d) Configuration settings will be monitored and under change control in accordance with established policies and procedures.

[CM-7] LEAST FUNCTIONALITY

Systems will be configured so that:

a) Only essential capabilities will be provided.
b) Should any such protocols be identified, System Owner will maintain a central list of prohibited ports, protocols, and/or services which may not be approved under any circumstances.
    - Under this policy, the following list of protocols is eligible for possible use; no unlisted protocol may be approved other than:

0 – HOPOPT	41 – IPv6	58 – IPv6-ICMP
1 – ICMP	43 – IPv6-Route	59 – IPv6-OPTS
4 – IPv4	44 – IPv6-Frag	135 – Mobility Header
6 – TCP	50 – ESP	139 – HIP
17 – UDP	51 – AH	140 – Shim6

    - Access to the following ports/services are prohibited to all systems without exception

Port Number	TCP	UDP
0	Reserved	Reserved
1	Tcpmux	tcpmux
2	Compressnet	compressnet
3	Compressnet	compressnet
4	Unassigned	unassigned
5	Rje	rje
6	Unassigned	unassigned
7	Echo	echo
8	Unassigned	unassigned
9	Discard	discard
10	Unassigned	unassigned
11	Systat	systat
12	Unassigned	unassigned
13	Daytime	daytime
14	Unassigned	unassigned
15	Unassigned	unassigned
16	Unassigned	unassigned
17	Qotd	qotd

18	Msp	msp
19	Chargen	chargen
512	Exec	comsat
513	Login	who
514	Shell	

[ENHANCED] [CM-7 (1)] PERIODIC REVIEW

Collaboratory will review the configuration of each information system such that:

a) Reviews will occur no less frequently than once every 15 months with an intended annual cadence to identify unnecessary and/or insecure functions, ports, protocols and services.
b) Any unnecessary or non-secure function, port, protocol and service will be disabled following the proper process for reconfiguration of the system (as provided for above).

[ENHANCED] [CM-7 (2)] PREVENT PROGRAM EXECUTION

Information systems will prevent program execution in accordance with rules authorizing the terms and conditions of software program usage for Collaboratory.

[ENHANCED] [CM-7 (4)] UNAUTHORIZED SOFTWARE / BLACKLISTING

Through the mandatory use of approved anti-malware software on all platforms supporting it:

a) Information systems will automatically identify and block software programs which are not authorized to execute on Collaboratory systems.
b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and
c) Blacklists will be updated by the anti-malware vendor and additional block lists (as required) will be maintained and reviewed at least once every 15 months, with an expected annual cadence.

[CM-8] INFORMATION SYSTEM COMPONENT INVENTORY

The Collaboratory will maintain:

a) An inventory of all information system components:
    1. Which accurately reflects the current information system;
    2. Includes all components within the authorization boundary of the information system;
    3. Is at the level of granularity deemed necessary for tracking and reporting;
    4. Includes location, serial number, memory amounts, processor types and speeds, internal storage components, and a listing of peripheral devices;
b) The inventory will be updated upon any hardware changes; whenever software installation or uninstallation occurs; whenever equipment is moved to a new location; and will be confirmed to be accurate independently of such functions at least once every 15 months with an expected annual cadence.

[ENHANCED] [CM-8 (1)] UPDATES DURING INSTALLATIONS / REMOVALS

The Collaboratory will update the inventory of information system components as an integral part of component installation, removals, and information system updates.

[ENHANCED] [CM-8 (3)] AUTOMATED UNAUTHORIZED COMPONENT DETECTION

Collaboratory will monitor systems to detect unauthorized components.

a) Automated inventory software will be selected, installed, and configured to run at least once monthly to detect what software and hardware is installed and report via the network to a central reporting location.
b) Upon detection of an unauthorized component, system managers will be notified.

[ENHANCED] [CM-8 (5)] NO DUPLICATE ACCOUNTING OF COMPONENTS

All components within the authorization boundary of the information system are counted only once in organizational inventories to ensure a correct accounting of hardware and software inventories, even in complex and interconnected systems.

[ENHANCED] [CM-9] CONFIGURATION MANAGEMENT PLAN

Collaboratory will generate specific configuration management procedures and metrics for all systems of moderate assurance or higher.

a) System managers are responsible for documenting configuration management procedures and will submit those procedures to System Owner for review prior to system authorization;
b) The procedures must establish a process to identify configuration items throughout the system development life cycle which will be managed as part of system configuration (for example, memory, non-volatile data storage, number/speed/type of central processing unit cores, bandwidth allocation);
c) Defines the configuration items for information systems and places those items under configuration management;
d) Protects the configuration management plan from unauthorized disclosure and modification.

[CM-10] SOFTWARE USAGE RESTRICTIONS

Software installed on Collaboratory information systems will conform to all relevant Federal, state, local and contractual legal requirements. To this end, the Collaboratory will:

a) Comply with all license agreements, terms of use, and the laws of copyright and patent in relation to Collaboratory's usage of software;
b) Track the use and installation of software and associated documentation. For software and documented protected by volume or quantity-based licenses to control copying and distribution, actual use will be at or below the licensed number of rights to use;

c) Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance or reproduction of copyrighted work.

[CM-11] USER-INSTALLED SOFTWARE

Except as described in system-specific documentation, users are explicitly not permitted to install any software on organizational information systems – such privileges shall be reserved for system managers on production systems, and to system managers and developers on test/development systems. This policy is should not be taken to prohibit personalization or configuration of user-level preferences that enhance productivity, workflow, or quality of work, except in so far as such user-level changes might affect organizational risk.

a) Exceptions may be authorized on user-system combinations based on a clear business need described and documented, when such implementations meet the requirements of least privilege/least functionality/most limited impact sufficient to both meet the business need and without shifting the risk profile in an unacceptable manner.
b) Software installation limitations will be enforced through operating system security measures.
c) Systems will be checked for unauthorized software and ineffective software installation controls at least once every 15 months, with an intended annual cadence.

CONTINGENCY PLANNING

[CP-1] CONTINGENCY PLANNING POLICY AND PROCEDURES

Collaboratory will draft one or more contingency plans with associated procedures. Plans will be designed in a modular manner, so that procedures and processes can be reused as much as possible to reduce the training, maintenance, and testing overhead of incident response.

a) These policies and procedures are to be disseminated to System Managers, Incident Response Managers, Developers, System Owner, and Security roles and, as needed, integrated into training provided to all other Collaboratory personnel.
b) All Contingency Planning Policies and Procedures must undergo periodic review to ensure that plans can be executed and that incident responses meet organizational needs, such that
    1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.
    2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle.

[CP-2] CONTINGENCY PLAN

Contingency planning for information systems is part of an overall organizational program for achieving continuity of System Owner for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of System Owner desired. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. Toward this end, the organization will:

a) Develop a contingency plan for the information system that:
    1. Identifies essential missions and business functions and associated contingency requirements;
    2. Provides recovery objectives, restoration priorities, and metrics;
    3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by System Owner or the line of business owner.

b) Distributes copies of the contingency plan to identified individuals who plays a role in the contingency plan and, as needed, is reflected in training provided to other parts of the organization affected if a system goes into a contingency mode;
c) Coordinates contingency planning activities with incident handling activities;
d) All contingency plans must undergo periodic review to ensure that plans can be executed and that incident responses meet organizational needs with a mandatory documentation review every 15 months with a preferred 1-year cycle, and with a mandatory tabletop walk-through (or actual event or exercise) once every 39 months with a preferred 3-year cycle.
e) Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f) Any changes to incident response plans will be communicated to all affected individuals within the Collaboratory; and
g) Protects the contingency plan from unauthorized disclosure and modification.

[ENHANCED] [CP-2 (1)] COORDINATE WITH RELATED PLANS

Contingency plan development must be coordinated with organizational elements responsible for related plans, such as incident response.

[ENHANCED] [CP-2 (3)] RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

Collaboratory will resume essential functions in a timely manner consistent with the criticality of the disrupted function. Prioritization must occur as part of the planning function.

[ENHANCED] [CP-2 (8)] IDENTIFY CRITICAL ASSETS

Collaboratory will identify critical information system assets supporting essential missions and business functions.

[CP-3] CONTINGENCY TRAINING

All System Managers, Incident Response Managers, Developers, System Owner and Security role holders will undertake contingency training approved by the Collaboratory (including internal training) consistent with their roles in contingency activities:

a) Training will be completed within 90 days of undertaking a contingency response role; preferably, training will occur prior to beginning a role where contingency response responsibilities must be undertaken.
b) Training will also occur within 30 days of information system, policy, procedure or plan changes.
c) Refresher/retraining will occur within 39 months, with a preferred 3-year cycle.

[CP-4] CONTINGENCY PLAN TESTING

Collaboratory will establish a testing protocol for all contingency plans and procedures, so that:

a) each plan is reviewed with at least a tabletop walk-through once every three years, to determine effectiveness and readiness to execute the plan;
b) Results must be documented in a report which must be reviewed by Security and System Owner;
c) Any corrective actions must be initiated as part of the review process.

[ENHANCED] [CP-4 (1)] COORDINATE WITH RELATED PLANS

Contingency plan testing will be coordinated to the extent possible with business continuity, incident response, and disaster recovery plan testing.

[ENHANCED] [CP-6] ALTERNATE STORAGE SITE

To address the potential risk of a loss of facilities by any number of disasters (including temporary weather-based disasters), Collaboratory will:

a) Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b) Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

[ENHANCED] [CP-6 (1)] SEPARATION FROM PRIMARY SITE

Collaboratory will identify one or more alternate storage sites that are separated from the primary storage site to reduce susceptibility to the same threats.

[ENHANCED] [CP-6 (3)] ACCESSIBILITY

Collaboratory will identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

[ENHANCED] [CP-7] ALTERNATE PROCESSING SITE

To address the potential risk of a loss of facilities by any number of disasters (including temporary weather-based disasters), Collaboratory will:

a) Establish an alternate processing site including necessary agreements to permit the transfer and resumption of all essential business functions within the recovery time and recovery point objectives identified with all essential business functions when the primary processing capabilities are unavailable;
b) Ensure that equipment and supplies required to transfer and resume System Owner are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c) Ensure that the alternate processing site provides information security safeguards equivalent to those of the primary site.

[ENHANCED] [CP-7 (1)] SEPARATION FROM PRIMARY SITE

Collaboratory will identify one or more alternate processing sites that are separated from the primary processing site to reduce susceptibility to the same threats.

[ENHANCED] [CP-7 (2)] ACCESSIBILITY

Collaboratory will identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

[ENHANCED] [CP-7 (3)] PRIORITY OF SERVICE

Collaboratory will develop alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

[ENHANCED] [CP-8] TELECOMMUNICATIONS SERVICES

Collaboratory will establish alternate telecommunications services including necessary agreements to permit the resumption of all essential business functions within that function's recovery time objective when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

[ENHANCED] [CP-8 (1)] PRIORITY OF SERVICE PROVISIONS

Because events which are capable of disrupting Collaboratory's normal System Owner could easily affect other organizations and entities within the region, Collaboratory will

a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).
b) Request Telecommunications Service Priority for all telecommunications services used for government functions affecting emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier, should such circumstances occur.

[ENHANCED] [CP-8 (2)] SINGLE POINTS OF FAILURE

Collaboratory will obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

[CP-9] INFORMATION SYSTEM BACKUP

System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Toward this end, Collaboratory will:

a) Conduct backups of user-level information contained in the information system with sufficient frequency and depth to meet recovery time and recovery point objectives for all systems;

b) Conduct backups of system-level information contained in the information system with sufficient frequency and depth to meet recovery time and recovery point objectives for all systems;
c) Conduct backups of information system documentation including security-related documentation with sufficient frequency and depth to meet recovery time and recovery point objectives; and
d) Protect the confidentiality, integrity, and availability of backup information at storage locations.

[CP-9 (1)] TESTING FOR RELIABILITY / INTEGRITY

Collaboratory will test backup information at least once per year to verify media reliability and information integrity. Backup mechanisms will check and report on integrity during the backup process to identify failing media.

[CP-10] INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Collaboratory provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

[ENHANCED] [CP-10 (2)] TRANSACTION RECOVERY

Collaboratory information systems will implement transaction recovery for systems that are transaction-based.

IDENTIFICATION AND AUTHENTICATION

[IA-1] IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Identification and authentication represent perhaps the most important methods to determine who is using information system resources, so that activities can be properly authorized.

a) Absent other specific guidance, it is the policy that all users will be identified and authenticated prior to being authorized to use any non-public system or access any non-public data.
    1. Human Resource and System Owner can perform IA functions described in IA-4, below. System managers are responsible for checking with Human Resources and System Owner prior to creating accounts or linking identities to authentication credentials.
    2. Absent other, more specific guidance, system managers will obtain written (emailed) authorization from Human Resources or System Owner as described in IA-4, specifically directing individuals have access.
b) All Identification and Authentication Policies and Procedures must undergo periodic review, such that
    1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.
    2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle

[IA-2] IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

All information systems will uniquely identify and authenticate organizational users or processes acting on behalf of organizational users. The act of a person or system interacting on behalf of an organizational user with a Collaboratory system will rely upon some form of technical credential prior to access being granted, in accordance with access control policies.

Technical credentials will be selected in accordance with the highest documented risk profile associated with an information system or the data stored on that system. Such credentials may include username/password combinations, physical tokens or other access codes. Biometric measurements may be utilized. Time and place based authentication may be used in addition to other credentials, based on specific risk profiles involved.

[IA-2 (1)] [IA-2 (2)] NETWORK ACCESS TO PRIVILEGED ACCOUNTS

Information systems will require multifactor authentication for network access to privileged accounts.

[ENHANCED] [IA-2 (2)] NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

Information systems will require multifactor authentication for network access to non-privileged accounts.

[ENHANCED] [IA-2 (3)] LOCAL ACCESS TO PRIVILEGED ACCOUNTS

Information systems will require multifactor authentication for all privileged access accounts, even local access.

[ENHANCED] [IA-2 (8)] NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT

Information systems will require the use of network access technologies which are resistant to network replay attacks for any remote network access to privileged accounts.

[ENHANCED] [IA-2 (11)] REMOTE ACCESS - SEPARATE DEVICE

Hardware tokens will be utilized in the authentication process for remote access to privileged systems. Tokens will be selected based on a risk profile for specific systems requiring remote access.

[IA-2 (12)] ACCEPTANCE OF PIV CREDENTIALS

Should Collaboratory implement PIV systems, said systems will be implemented in compliance with FIPS-201 to support information system use.

[ENHANCED] [IA-3] DEVICE IDENTIFICATION AND AUTHENTICATION

Remote access connections to non-public systems will be authenticated by the use of system-specific strong cryptography.

[IA-4] IDENTIFIER MANAGEMENT

For any account that is not Anonymous or Guest (that is, public in nature):

a) Authentication credentials will be authorized by the Human Resources or System Owner functions. Prior to authorization, the identity of the recipient must be confirmed by checking government-issued photo identification by the authorizing party.
b) System managers will select unique identifiers to the individual.
c) System managers will assign unique identifiers to the individual.
d) Unique identifiers may not be re-used for a minimum of 6 months following account termination, unless re-issuance is to the same individual.
e) Unique identifiers will be suspended or disabled after 21 days of inactivity

[IA-5] AUTHENTICATOR MANAGEMENT

a) System managers will issue credentials using secure data transfer directly to recipients only if they have received written authorization (email is sufficient) from an authorizing function. In addition, the credential issuing function will be cross-checked by Human Resources or System Owner who verbally confirms they have checked the photo identification of the recipient in the physical presence of both the system manager and the recipient, or when the system manager personally checks the organizationally issued photo identification of the recipient.
b) Collaboratory will document and enforce minimum strength requirements initial authentication processes for any non-public system.

c) On a system-by-system basis, strength of authentication mechanisms will be evaluated to ensure appropriateness for the intended use.

d) Collaboratory will document and follow system-specific procedures for credential distribution. Absent specific procedures:
   - Initial distribution of credentials will occur in person only with identification checks.
   - If a user reasonable believes his credentials to be lost or compromised, he will notify Collaboratory immediately so that the account access can be suspended. Reset credentials should be issued in person using the same processes as initial distribution; however, if risk levels and business needs permit, by out-of-band mechanisms (telephone, SMS) if the system manager and his direct supervisor agree that there is reasonable assurance that the identity of the individual is confirmed and that the credential has not been/will not be compromised in transit.

e) Factory default authenticators will be changed prior to systems being made accessible to users, for remote access login, or in any way outside tightly controlled integration and testing environments.

f) Barring system-specific documentation that provides a risk assessment profile and business justification to the contrary, credentials must be refreshed on the following schedule. No credential type may be utilized for authorized purposes without being documented in section IA-5g below.

g)

Credential Type	Minimum life	Maximum Life	Reuse Conditions
System Password	Single use	1827 days	No reuse within 731 days of last change
SSL Certificate	30 days	1827 days	No reuse
Cryptographic private key unlock password	1 year	1827 days	No reuse
Biometric		1827 days	Reuse permitted based on refreshed measurement.

h) Barring system-specific documentation that provides a risk assessment profile and business justification to the contrary, password credentials will be stored in cryptographically protected containers that are powered by one-way hashing functions. Cryptographic private keys will be stored in a “locked” password protected form.

i) Collaboratory will prepare training and procedures for the protection of credentials so that Collaboratory users will be able to safeguard their credentials.

j) Group/Role accounts will have credentials changed whenever group membership changes to remove an authorized individual.

[IA-5 (1)] PASSWORD-BASED AUTHENTICATION

Single factor authentication, particularly of the username/password variety, is a particularly weak form of authentication as a result of the capabilities and change rates in modern computing technology. As a result, the following password strength restrictions should be reviewed for technical adequacy at least once every 15 months, with an intended cadence of at least once per year, and within 30 days of a technical development affecting speed of password "cracking" become widely known.

a) User-selected passwords will represent a minimum of 128 bits of randomness or:
   - Have a minimum length of 12 characters
   - Contain at least one upper, one lower, one numeric, and one special (punctuation) character
   - Not fall within any Collaboratory-approved password dictionary, including common symbol-for-character swaps in that dictionary
   - Not utilize any keyboard, numeric, alphabetical, or other widely predictable sequences of 4 or more characters.

b) When a password is changed, a minimum of 5 characters must change. Those changes must have each of the following three characteristics:
   - Change at least one character in the first 5 bytes of the password
   - Change at least one character in the last 5 bytes of the password
   - Change at least one character that is not in either the first 5 or last 5 characters.

c) Systems must store passwords in a cryptographically protected form only

d) As noted in IA-5, passwords may be kept for periods up to 1827 days (5 years). Passwords must additionally be changed if they are suspected to be compromised. Systems should alert system managers whenever more than 1 password change occurs within a 7-day period.

e) As noted in IA-5, passwords must not be reused within 731 days of the last change or within the previous 3 passwords, whichever comes **last**.

f) Systems will permit the use of (pseudo)randomly generated passwords for temporary use which result in immediate and mandatory changes to the permanent password.

[ENHANCED] [IA-5 (2)] PKI-BASED AUTHENTICATION

The information system, for PKI-based authentication:

a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

b) Enforces authorized access to the corresponding private key;

c) Maps the authenticated identity to the account of the individual or group; and

d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

[ENHANCED] [IA-5 (3)] IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION

Authorization to receive system credentials (usernames, passwords, tokens, certificates, etc.) will come from Human Resources or System Owner. As part of the initial registration process, said authority will check a government-issued photo ID to confirm the identity of the credential recipient. Authorization to proceed will be communicated in writing to appropriate system managers, and ID will be checked again by system managers or, only if the system manager, recipient, and authorizing function are able to be physically present in the same location, verbally confirmed by the authorizing authority.

[IA-5 (11)] HARDWARE TOKEN-BASED AUTHENTICATION

Should token-based authentication be issued, specific requirements will be drafted prior to their being put into production use.

[IA-6] AUTHENTICATOR FEEDBACK

Information systems will be configured to obscure feedback of authentication information during the authentication process.

[IA-7] CRYPTOGRAPHIC MODULE AUTHENTICATION

Should cryptographic module authentication be used, information systems will implement mechanisms for authentication to a cryptographic module that meet all applicable Federal, state, local and contractual legal requirements.

[IA-8] IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Information systems will uniquely identify and authenticate non-organizational users.

[IA-8 (2)] ACCEPTANCE OF THIRD-PARTY CREDENTIALS

Information systems will not accept third-party credentials.

[IA-10] ADAPTIVE IDENTIFICATION AND AUTHENTICATION

The organization requires that individuals accessing the information system employ secondary authentication or multi-factor authentication whenever privilege escalation is required or under specific circumstances or situations defined in system specific documentation. Any such documentation will describe the situation that requires additional identification and authentication, what measures are required, and what concerns it helps to mitigate.

[IA-11] RE-AUTHENTICATION

Users and devices will re-authenticate under the following conditions:

- To end a session lock
- At least once every 6 hours of use for interactive sessions
- At least once every 8 hours for devices

INCIDENT RESPONSE

[IR-1] INCIDENT RESPONSE POLICY AND PROCEDURES

Collaboratory will draft one or more incident response plans with associated procedures, ensuring that each information system is under the governance of one and only one incident response plan. Plans will be designed in a modular manner, so that procedures and processes can be reused as much as possible to reduce the training, maintenance, and testing overhead of incident response.

a) These policies and procedures are to be disseminated to System Managers, Incident Response Managers, Developers, System Owner, and Security roles.
b) All Incident Response Policies and Procedures must undergo periodic review to ensure that plans can be executed and that incident responses meet organizational needs, such that
    1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.
    2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle.

[IR-2] INCIDENT RESPONSE TRAINING

All System Managers, Incident Response Managers, Developers, System Owner and Security role holders will undertake incident response training approved by the Collaboratory (including internal training) consistent with their roles in incident response activities:

a) Training will be completed within 90 days of undertaking an incident response role; preferably, training will occur prior to beginning a role where incident response responsibilities must be undertaken.
b) Training will also occur within 30 days of information system, policy, procedure or plan changes.
c) Refresher/retraining will occur within 39 months, with a preferred 3-year cycle.

[IR-3] INCIDENT RESPONSE TESTING

Collaboratory will establish a testing protocol for all incident response plans and procedures, so that each plan is reviewed with at least a tabletop walk-through once every three years, to determine effectiveness. Results must be documented in a report to Security and System Owner that provides for process improvement over time.

[ENHANCED] [IR-3 (2)] COORDINATION WITH RELATED PLANS

Incident response testing will be coordinated to the extent possible with business continuity, contingency, and disaster recovery plan testing.

[IR-4] INCIDENT HANDLING

Collaboratory will develop an incident response capability that can be activated swiftly in response to security issues. The capability will be operationally managed through the Security function, and will be drawn from trained individuals who are contractors to or employees of the Collaboratory. The

Collaboratory will maintain current contact information in for all current and potential members of the incident response capability.

a) The key functions of incident handling will include:
    - Analysis of and commenting on response plans for individual systems
    - Intelligence gathering, including threat/vulnerability assessment and incident detection
    - Evidence collection, preservation, and analysis
    - Containment, Mitigation, Eradication and Remediation planning and implementation
    - Legal, financial, and organizational risk advisory functions
    - Communication and information outflow management, including interaction with external security organizations and law enforcement.
b) Incident response handling activities will be coordinated with contingency planning activities.
c) Any security incident will prompt review and revision of incident response procedures, training and testing to incorporate lessons learned from ongoing incident handling. Any incident resulting in moderate or higher legal, financial or organizational risk must be reported to the Executive upon determination of that risk.

[ENHANCED] [IR-4 (1)] AUTOMATED INCIDENT HANDLING PROCESSES

Collaboratory will select and implement automated systems to support the incident handling process.

[IR-5] INCIDENT MONITORING

The Incident Response Manager will track and document information system security incidents and will be given access and cooperation from all system managers to ensure access to appropriate information. The Incident Response manager will inform risk assessment processes upon request based on current organizational experience and intelligence gathering activities.

[IR-6] INCIDENT REPORTING

Incident reporting will be reflected in both public and internal Collaboratory Terms of Use. Collaboratory training will also include incident reporting training for all users.

a) All Collaboratory users (including public/anonymous users) are required to report suspected security incidents affecting Collaboratory systems or data (including on systems used to access non-public Collaboratory systems and data).
b) Collaboratory will designate a security point of contact and will ensure that all reports of suspected incidents are directed there. Absent other guidance, the security point of contact will be the Incident Response Manager.

[ENHANCED] [IR-6 (1)] AUTOMATED REPORTING

Collaboratory will utilize automation to assist in the reporting of security incidents.

[IR-7] INCIDENT RESPONSE ASSISTANCE

Collaboratory will offer advice and assistance to users of the information system for the handling and reporting of security incidents through system managers and technical support capabilities.

[ENHANCED] [IR-7 (1)] AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT

Collaboratory will employ automation to increase the availability of incident response-related information and support.

[IR-8] INCIDENT RESPONSE PLAN

Collaboratory will:

a) Maintain incident response planning documentation and training
    1. Incident response plans will be will be split to address specific organizational needs but scoped as broadly as possible to minimize complexity. Any incident response plan will address each of the following stages of an incident:
        - Preparation: including team makeup; call lists and communication points; explicit authority to search systems and monitor traffic; how to authorize outreach to external security organizations and law enforcement; evidence preservation requirements; uncommon procedures to access data (forensic techniques, access to audit logs, access to non-information system data sources such as video surveillance systems and card access logs); and the personnel, information systems, and data under the scope of the incident response plan.
        - Identification: including mechanisms to detect and receive reports about security incidents.
        - Containment: specifically identifying who can authorize isolation or the disruption of operation of an impacted system; what level of evidence preservation is required (and whether appropriate training/certification is available); what levels of access are required to perform that containment; and a checklist of what information to collect and who to notify prior to containment actions occurring.
        - Eradication: must include procedures identify the vulnerable software/component that was exploited, and to identify other affected systems within the Collaboratory.
        - Recovery: must include an authorization process which can return a system to operation covering all of the following scenarios: (a) a patch to address the vulnerability is available, (b) if a patch is not available but technical mitigation through configuration or additional software is available, or (c) no such mitigation is available; monitoring for affected systems following return to service; and end-user validation testing prior to return to service.

- Lessons Learned: must include post-incident review and analysis, including a "hot wash" within the first 24 hours to capture issues and concerns while experience and perceptions are fresh, and within the first 7 days to see longer-term issues. The lessons learned process must report on:
    - what went right, as well as gaps or failures, both of the plan and of execution/implementation of the plan;
    - whether communication plans and preparations were sufficient;
    - whether sufficient resources and staff were allocated to the incident response capability in the specific case;
    - whether additional training (or a tabletop or functional exercise of the incident response capability) is required or beneficial;
    - effectiveness of existing tools for incident response;
    - whether additional or updated tools would improve the timeliness or quality of the response;
    - Whether any existing policies, procedures, processes, training, or implementation of information systems could be improved to reduce the probability or impact of future security incidents from an organizational perspective.

2. The Incident Response Capability will be under the tactical command of an Incident Response Manager, with affected system managers and developers staffing the team for technical response. The incident response capability will collaborate with external communications functions, and provide technical risk assessment information, which can be combined with organizational legal, financial and organization risk expertise.
3. The Incident Response Manager reports to Security, who in turn reports to the Executive. Incident response must not be under the same organizational authority as system managers.
4. Any unique requirements of the Collaboratory must be documented to be followed.
5. A security incident is defined as the discovery of critical vulnerabilities in Collaboratory information systems or actual exploitation of those critical vulnerabilities. A critical vulnerability can or does result in: the control of an information system or process shifting to any party other than the authorized user; loss of critical functionality; unauthorized change(s) to system configuration, software, data, or behavior; or the disclosure of non-public data to an unauthorized party.
6. Incident response capabilities will track the number of incidents reported; number of reports which do not qualify as incidents; and time from report/detection to containment, to eradication, and to recovery. The number of man-hours for each member of the incident response team dedicated to each incident will also be recorded.
7. Incident response plans must identify the resources and management support needed to effectively maintain and mature an incident response capability

8. The incident response capability will be reviewed by Security and approved by System Owner.

b) Distribute copie of the plan to system managers, developers, System Owner, and Security; training on how and assessing when to contact incident response will be available to all users.
c) Perioidically review all Incident Response plans to ensure that plans can be executed and that incident responses meet organizational needs with a mandatory documentation review every 15 months with a preferred 1-year cycle, and with a mandatory tabletop walk-through (or actual event or exercise) once every 39 months with a preferred 3-year cycle.
d) Update incident response plans and associated training materials to address any system/organizational changes, or problems encountered during plan implementation, execution, or testing.
e) Communicate any changes to incident response plans to all affected individuals within the Collaboratory.
f) Protect incident response plans from unauthorized disclosure and modification.

MAINTENANCE

[MA-1] SYSTEM MAINTENANCE POLICY AND PROCEDURES

Collaboratory will maintain general policies and procedures governing system maintenance, and may implement stronger policies for specific systems or groups of systems.

a) Maintenance Policies and Procedures will be distributed to System Managers and govern their work.

b) All System Maintenance Policies and Procedures must undergo periodic review, such that

1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.

2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle

[MA-2] CONTROLLED MAINTENANCE

All maintenance work will be governed and executed in accordance with a policy of retaining maximum control of systems and data even during maintenance, such that:

a) Collaboratory will schedule, perform, document and review records of maintenance and repairs on information system components in accordance with the strictest of: manufacturer specifications, vendor specifications, organizational requirements, or industry best practice.
b) Collaboratory will approve and monitor all maintenance activities, whether performed on site or remotely and whether equipment is serviced on site or removed to another location.
c) System Managers must perform a risk assessment and obtain the approval of their direct supervisor prior to removal of the information system or system components from organizational facilities for off-site maintenance or repair.
d) Systems will be sanitized to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repair.
e) System Managers will check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
f) Organizational maintenance records will be maintained, reflecting date, time, party performing maintenance, and maintenance tasks performed for all Collaboratory information systems and component for the life of any affected components.

[ENHANCED] [MA-3] MAINTENANCE TOOLS

Collaboratory will approve, control, and monitor information system maintenance tools which are not part of the information systems themselves.

[ENHANCED] [MA-3 (1)] INSPECT TOOLS

Collaboratory will inspect any maintenance tools carried into the facility by maintenance personnel for improper or unauthorized modifications including but not limited to inclusion of malicious code.

[ENHANCED] [MA-3 (2)] INSPECT MEDIA

Collaboratory will check digital media containing diagnostic and test programs for malicious code prior to the media being used in the information system.

[MA-4] NONLOCAL MAINTENANCE

Non-Local maintenance tasks are performed by an individual not physically working at the console of a device, for example via a network. Because maintenance tasks can affect other users and the integrity, confidentiality, and availability of systems and data, for any non-local maintenance task, Collaboratory will:

a) Approve and monitor all nonlocal maintenance and diagnostic activities.
b) Ensure that all non-local maintenance and diagnostic tools are consistent with organizational policy and documented in the security plan for the information system.
c) Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions in accordance with IA-2 above.
d) Maintain records for nonlocal maintenance and diagnostic activities; and
e) Terminate session and network connections when nonlocal maintenance is completed.

[ENHANCED] [MA-4 (2)] DOCUMENT NONLOCAL MAINTENANCE

Collaboratory will document in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

[MA-5] MAINTENANCE PERSONNEL

Only authorized personnel will perform maintenance on Collaboratory information systems. To this end, Collaboratory will:

a) Maintain a list of authorized maintenance personnel and organizations, which will be approved by System Owner prior to maintenance being performed.
b) Ensure that any non-escorted personnel performing maintenance on the information system have required access authorizations; and
c) Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

[ENHANCED] [MA-6] TIMELY MAINTENANCE

Collaboratory will have spare parts and components available or will have a contract in place to obtain said parts and components within the window of acceptable disruption to services should a component fail. For most Collaboratory systems, this will be 4 business days, but may be shorter or longer based on

the criticality of the components. All systems will be identified as part of its risk assessment as to how much disruption is acceptable to services it offers and will be resourced accordingly.

MEDIA PROTECTION

[MP-1] MEDIA PROTECTION POLICY AND PROCEDURES

Collaboratory will maintain general policies and procedures governing media protection, and may implement stronger policies for specific classifications of data stored on media.

a) Media protection policies and procedures will be distributed to any Collaboratory personnel having physical access to media containing non-public information and shall govern their work.

b) All Media Protection Policies and Procedures must undergo periodic review, such that

   1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.

   2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle

[MP-2] MEDIA ACCESS

Information system media includes both digital (magnetic media of any types, optical disks, removable or portable hard drives, USB flash drives, etc.) and non-digital (e.g. paper, film, microfilm) formats. Media containing any non-public data will be restricted to a need-to-know, need-to-use basis for the completion of authorized work.

[ENHANCED] [MP-3] MEDIA MARKING

Non-public data stored on information system media must be labelled to facilitate proper handling.

a) Markings on information system media will indicate the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
b) Digital media and non-digital media are exempt from the marking requirement as long as the media remains within Collaboratory facilities in locked rooms, such as private offices where doors are routinely closed and locked when unattended or the SCILL laboratory.

[ENHANCED] [MP-4] MEDIA STORAGE

Media will be retained in approved secure Collaboratory storage facilities in accordance with the data classification. Media containing data of high sensitivity will be checked in and out of that facility.

a) Physically controls and securely stores all digital media containing non-public information in areas specifically identified in the data inventory as being authorized locations.
b) Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

[ENHANCED] [MP-5] MEDIA TRANSPORT

Media transport refers to the transportation of information system media outside of Collaboratory controlled facilities where sufficient physical and procedural controls are in place to protect the media and the data stored upon it from disclosure, corruption or loss. Media transport concerns itself with both digital and non-digital media, and mobile computing devices such as laptops, tablets, smartphones, and e-readers.

a) Collaboratory personnel in possession of information system media that contains any non-public information will utilize appropriate safeguards for that media, such as ensuring that non-public information remains encrypted while in transit and that non-digital media are stored in containers which resist attempts at access to the media or the information upon it in accordance with the data classification and risk profile.
b) Collaboratory personnel will maintain accountability for information system media during transport outside of controlled areas.
c) Media in transit will be tracked and activities surrounding the media documented to prevent and detect loss, destruction or tampering in accordance with the data classification and risk profile of the data.
d) Only authorized Collaboratory personnel or authorized courier entities may transport information system media outside of controlled facilities.

[ENHANCED] [MP-5 (4)] CRYPTOGRAPHIC PROTECTION

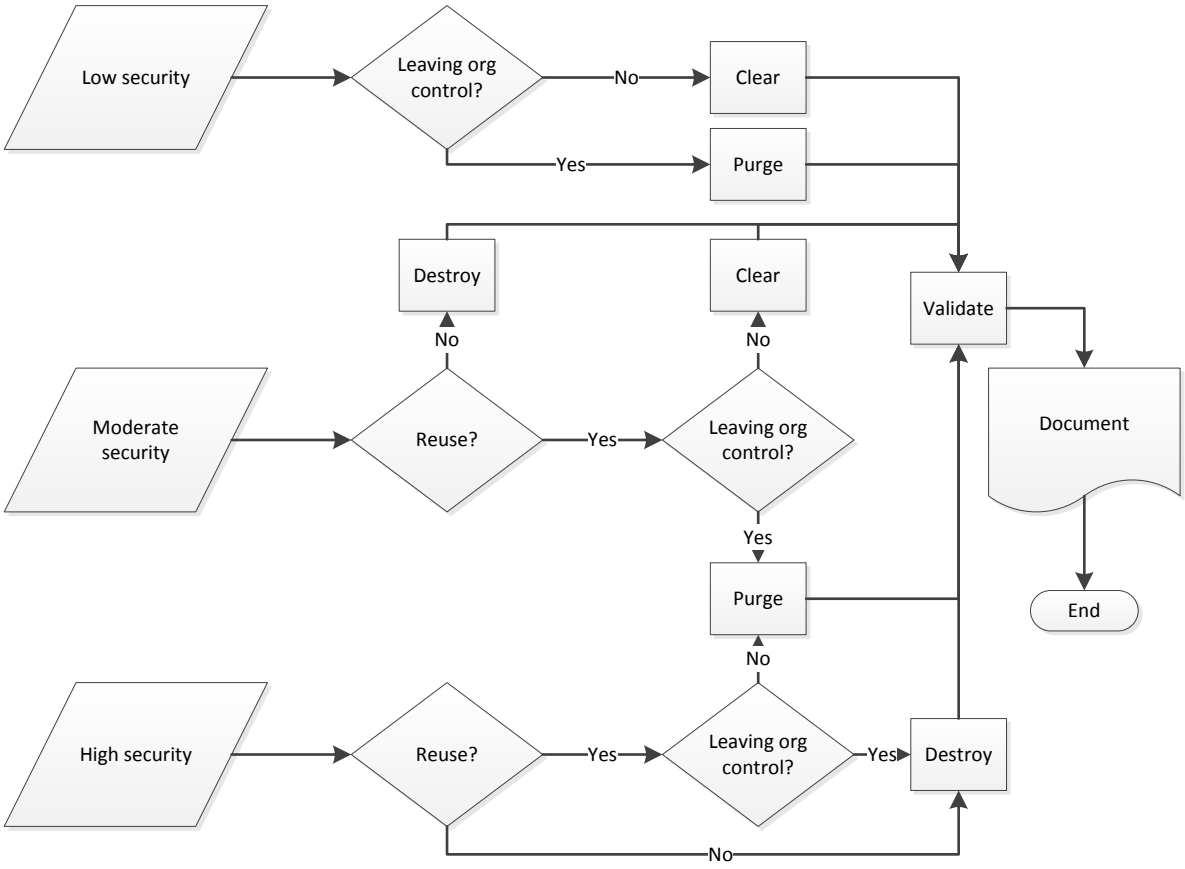
All digital information system media that carries sensitive data will be utilize the strongest available cryptographic protection mechanisms in accordance with the data classification to protect the confidentiality and integrity of information stored on the digital media during transport outside of controlled areas.

[MP-6] MEDIA SANITIZATION

Information system media will be sanitized prior to being released for disposal or reuse will undergo sanitization, such that the information on the media is fully public or explicitly intended for the recipient.

a) Information system media may be destroyed via shredding or Collaboratory approved media destruction services. Erasure for repurposing or release outside the organization will conform to the guidance of NIST special publication 800-80.

b) Collaboratory will employ media sanitization mechanisms that provide data destruction with an assurance level commensurate with the security classification of the device or data involved.



[MP-7] MEDIA USE

Collaboratory restricts the use of portable information system media by data and system classification. Appropriate media authorizations by media characteristics must be documented and authorized in accordance with risk profiles.

Information System Media Characteristics	Examples
Digital, read-only	CD/DVD/BD ROM
Digital, limited write	CDR/CDRW, DVDR/RW, BDR/RW
Digital, read-write	Hard disk, flash drives, external drives
Non-digital, read-only	Scanner-friendly documents
Non-digital, write-only	Paper

[ENHANCED] [MP-7 (1)] PROHIBIT USE WITHOUT OWNER

The use of portable storage devices in Collaboratory information systems is expressly prohibited when such devices have no identifiable owner.

PHYSICAL AND ENVIRONMENTAL PROTECTION

[PE-1] PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Collaboratory will adopt or maintain general policies and procedures governing physical and environmental protection. Absent specific guidance, physical and environmental protection will at a minimum conform to the policies and procedures put into place by the management of leased facilities and may at Collaboratory's discretion use additional protections to address organization-specific risk.

a) Physical and environmental protection policies and procedures will be distributed to any Collaboratory personnel required to implement or execute said protection. Summaries, training, and other orientation will be provided to all Collaboratory personnel and to guests as required to conform to the policy.

b) All Physical and environmental protection Policies and Procedures must undergo periodic review, such that

   1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.

   2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle

[PE-2] PHYSICAL ACCESS AUTHORIZATIONS

To implement physical and environmental protection, Collaboratory will:

a) Develop, approve, and maintain a list of individuals with authorized access to the facility where information systems reside
b) Issue authorization credentials for facility access;
c) Review at least quarterly the access list detailing individuals' authorized facility access; and
d) Remove individuals from the facility access list when access is no longer required.

[PE-3] PHYSICAL ACCESS CONTROL

Physical access to Collaboratory facilities will be managed directly by Collaboratory or be caused to be managed under contractual terms in some leased facilities. Internal secured facilities within Collaboratory (e.g. SCILL) may have additional security measures. This control applies to Collaboratory employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Toward this end, Collaboratory will:

a) Enforce physical access authorizations at all intended entry points to secure facility areas by;
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using locked doors;
a) Maintain physical access audit logs for server facilities and SCILL;

b) Provide and utilize Collaboratory personnel and guest identification name tags to control access to areas within the facility officially designated as publicly accessible;
c) Escort visitors and monitor visitor activity;
d) Secure keys, combinations, and other physical access devices;
e) Inventory keys, combination assignments, keycards, and organization-issued IDs at least annually; and
f) Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated, or as mandated by Battelle Memorial Institute physical security/facilities.

[ENHANCED] [PE-4] ACCESS CONTROL FOR TRANSMISSION MEDIUM

Physical access to external distribution and transmission lines will be limited to prevent intentional or accidental disruptions, either directly by Collaboratory or managed by facilities leased by Collaboratory.

[ENHANCED] [PE-5] ACCESS CONTROL FOR OUTPUT DEVICES

Collaboratory will control physical access to information system output devices to prevent unauthorized individuals from obtaining the output. This will be accomplished by using only output devices within secure facilities when outputting sensitive data, or by having the output device attended by authorized Collaboratory personnel when the output is initiated.

[PE-6] MONITORING PHYSICAL ACCESS

Facilities leased by Collaboratory may manage physical access logging data for Collaboratory access. Internal secured facilities utilizing logging (e.g. SCILL) will have independently managed physical access controls. For internally managed logging, Collaboratory will:

a) Monitor physical access to secured facilities to detect and respond to physical security incidents;
b) Review physical access logs at least once per month and upon occurrence or indication of any security breach.
c) Coordinate physical access log reviews and investigations with Collaboratory's incident response capability.

[ENHANCED] [PE-6 (1)] INTRUSION ALARMS / SURVEILLANCE EQUIPMENT

Collaboratory will monitor physical intrusion alarms and surveillance equipment.

[PE-8] VISITOR ACCESS RECORDS

Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas. Collaboratory will:

a) Maintain visitor access records to the facility where the information system resides for a period of no less than 1 year and no more than a business-defined purpose or 3 years, whichever is longer; and
b) Review visitor access records at least quarterly.

[ENHANCED] [PE-9] POWER EQUIPMENT AND CABLING

Collaboratory will mitigate the probability and impact of damage and destruction for power equipment and cabling for information systems directly or through agreement terms with leased facilities..

[ENHANCED] [PE-10] EMERGENCY SHUTOFF

This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Either directly or through agreement terms with leased facilities, Collaboratory will:

a) Provide the capability of shutting off power to the information system or individual system components in emergency situations;
b) Place emergency shutoff switches or devices in appropriate power distribution facilities to facilitate safe and easy access for personnel; and
c) Protect emergency power shutoff capability from unauthorized activation.

[ENHANCED] [PE-11] EMERGENCY POWER

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of all critical information systems in the event of a primary power source loss.

[PE-12] EMERGENCY LIGHTING

Collaboratory will directly or through agreement terms with leased facilities employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

[PE-13] FIRE PROTECTION

Collaboratory will directly or through agreement terms with leased facilities employ and maintain fire suppression and detection devices/systems that are supported by an independent energy source.

[ENHANCED] [PE-13 (3)] AUTOMATIC FIRE SUPPRESSION

Collaboratory will directly or through agreement terms with leased facilities employ and maintain automatic fire suppression devices and systems.

[PE-14] TEMPERATURE AND HUMIDITY CONTROLS

This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms. Toward this end, Collaboratory either directly or through agreement terms with leased facilities will:

a) Maintain temperature and humidity levels within the facility within equipment manufacturer's documented acceptable tolerances; and

b) Monitor temperature and humidity levels.

[PE-15] WATER DAMAGE PROTECTION

Collaboratory will take reasonable and appropriate measures to prevent and mitigate water leakage damage to its computing facilities. At a minimum, any leased or owned facility will maintain master shutoff or isolation valves that are accessible, working properly, and have key personnel that are knowledgeable, trained, and have access to manage them.

[PE-16] DELIVERY AND REMOVAL

Collaboratory authorizes, monitors, and controls backup media and non-mobile information system components, including those used by third-party maintenance organizations, entering and exiting the facility and maintains records of those items.

[ENHANCED] [PE-17] ALTERNATE WORK SITE

Alternate work sites may include, for example, private residences of employees, hotel rooms, and day offices. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Collaboratory may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and facilitates telecommuting and other flexible work arrangements. Toward this end, Collaboratory will:

a) Develop, approve, and employ organization-defined security controls at alternate work sites;
b) Assess the feasibility and effectiveness of security controls at alternate work sites; and
c) Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

PLANNING

[PL-1] SECURITY PLANNING POLICY AND PROCEDURES

Collaboratory will maintain general policies and procedures governing security planning, and may implement stronger policies for specific information systems or data.

a) Security Planning policies and procedures will be distributed to any Collaboratory personnel responsible for the implementation, operation, maintenance, or evaluation of Collaboratory information systems and data.

b) All Security Planning Policies and Procedures must undergo periodic review, such that

1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.

2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle

[PL-2] SYSTEM SECURITY PLAN

Each information system will be documented, at a high level, describing the overall security requirements, controls the systems are subject to and how the implementation of the system meets those control objectives. In addition, security plans will contain sufficient information about assigned parameters to enable a design and implementation that unambiguously complies with the intent of the plans and subsequent determinations of risk. Effective security plans utilize extensive references to existing documentation such as policies, procedures, design and implementation specifications, and standards to reduce documentation requirements and simplify document management.

a) Collaboratory will develop information system specific security plans that:
   1. Are consistent with the organization's enterprise architecture;
   2. Explicitly define the authorization boundary for the system;
   3. Describe the operational context of the information system in terms of missions and business processes;
   4. Provide the security categorization of the information system including supporting rationale;
   5. Describe the operational environment for the information system and relationships with or connections to other information systems;
   6. Provide an overview of the security requirements for the system;
   7. Identify any relevant overlays, if applicable;
   8. Describe the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b) Copies of security plans will be distributed to system managers, developers, evaluators, and security personnel; changes to security plans will be communicated to the same.
c) Distributes copies of the security plan and communicates subsequent changes to the plan to Reviews the security plan for the information system at least once every 39 months with an intended minimum cadence of every 3 years or as prompted by changes to operational context;
d) Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
e) Protects the security plan from unauthorized disclosure and modification.

[ENHANCED] [PL-2 (3)] PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

Collaboratory plans and coordinates the scheduling and execution of security-related activities affecting the information system with system managers, evaluators, and System Owner and Security to reduce the impact on other organizational entities. Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination is intended to be inclusive of both emergency and non-emergency situations.

[PL-4] RULES OF BEHAVIOR

Terms of use/rules governing behavior on information systems will be provided to users and referenced or fully displayed in banner notifications as descried in AC-8 above. These rules will:

a) Establish and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b) Receive a signed acknowledgment (digital signature is acceptable if it can be logged or demonstrated to be consistently applied) from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c) Rules of behavior/terms of use will be reviewed after 3 months of operation or as part of the lessons learned phase of a security incident. In addition, rules of behavior will be evaluated at least once every 39 months, with an expected 3-year cadence.
d) Changes to rules of behavior require individuals who have signed a previous version of the rules of behavior to read and sign the new version.

[ENHANCED] [PL-4 (1)] SOCIAL MEDIA AND NETWORKING RESTRICTIONS

Collaboratory will include in its rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. Absent that guidance, discussion of any work-related matter on social media is expressly prohibited.

[PL-8] INFORMATION SECURITY ARCHITECTURE

Collaboratory will design and implement a coherent architecture for its information systems, which describes the layout, placement and allocation of security functionality (including security controls),

security-related information for external interfaces, information being exchanged across those interfaces, and the protection mechanisms associated with each interface. In addition, it will integrate with the security policy's description of roles and responsibilities, unique security requirements; types of information processed, stored and transmitted by information systems, service continuity and restoration priorities in a contingency situation, and any other specific protection needs. The security architecture will include baseline approved configurations for each operating system in use, which will be documented and under change control with approval processes under System Owner.

a) Toward this end, Collaboratory will develop an information security architecture for the information system that:
    1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
    2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
    3. Describes any information security assumptions about, and dependencies on, external services;
b) Collaboratory will review and update the information security architecture upon each new type of component being added to the collection of Collaboratory information systems and at least once every 39 months with an expected 3-year cadence to reflect updates in the enterprise architecture; and
c) Collaboratory will ensure that planned information security architecture changes are reflected in the security plan and organizational procurements/acquisitions.

PERSONNEL SECURITY

[PS-1] PERSONNEL SECURITY POLICY AND PROCEDURES

Collaboratory will maintain policies and procedures governing personnel security.

a) Personnel security policies and procedures will be distributed to human resource functions and to any supervisor having one or more direct reports within the Collaboratory.

b) All personnel security Policies and Procedures must undergo periodic review, such that

1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.

2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle

[PS-2] POSITION RISK DESIGNATION

Because internal personnel create the inherent possibility of subverting security functionality, and because internal personnel are inherently given trust and responsibility that affects the function of the organization:

a) Collaboratory will assign risk designations to all organizational positions;
b) Collaboratory will establish screening criteria for individuals filling those positions;
c) Review and update position risk designations at least once every calendar year.

[PS-3] PERSONNEL SCREENING

No part of the personnel screening policies and procedures supersedes Federal, state, local, or contracted legal requirements.

a) All individuals will be screened prior to authorizing access to information systems;
b) Screenings will be considered valid for a period of three years. New access authorizations after that validity period require rescreening. In the event of real or perceived security and policy breaches, rescreening is indicated.

[PS-4] PERSONNEL TERMINATION

Human resources are responsible for personnel termination functions. Upon termination of employment:

a) Human Resources will communicate to all information system managers within 1 hour of employment termination. Remote information system accessand Collaboratory wireless LAN access must be terminated within 1-hour of notification; every reasonable effort must be taken to ensure remote and local wireless access is terminated quickly as possible. All information system access will be terminated by system managers within one business day.

b) System managers will revoke or terminate any authenticators/credentials associated with the individual.
c) Human Resources will conduct an exit interview which discusses confidentiality, trade secret, Collaboratory intellectual property rights, and information and system access restrictions on data in the individuals' and Collaboratory's custody.
d) Collaboratory will collect all security-related organizational information system related property;
e) Collaboratory will retain access to organizational information and information systems formerly controlled by terminated individuals; and
f) Human Resources will notify all affected personnel within 1 business day.

[PS-5] PERSONNEL TRANSFER

Whenever a personnel transfer within the Collaboratory occurs, privileges and authorizations for that individual may also need to change. Toward that end, Human Resources will:

a) Review and confirm ongoing operational need for current logical and physical access authorizations to information systems and facilities when individuals are reassigned or transferred to other positions within the organization.
b) Direct system managers to, within one business day, correct logical and physical access authorizations for identifiers associated with the transferring individual.
c) System managers will modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer within two business days.
d) Notify all affected personnel of role changes within 1 business day.

[PS-6] ACCESS AGREEMENTS

Non-disclosure, acceptable use, rules of behavior, and conflict of interest agreements are examples of access agreements used to govern access to Collaboratory systems. Collaboratory will:

a) Develop and document access agreements for its information systems.
b) Review and as needed update all access agreement templates at least once every 39 months with an intended 3-year cycle.
c) Require individuals seeking access to Collaboratory systems to:
    1. Sign appropriate access agreements prior to being granted access
    2. Resign/refresh access agreements to maintain access whenever access agreements are updated or at least once per calendar year.

[PS-7] THIRD-PARTY PERSONNEL SECURITY

Third-party personnel refer to service bureaus, contractors, and Collaboratory member employees working with or on Collaboratory information systems in a non-public manner. Collaboratory will:

a) Establish personnel security requirements and classifications, including roles and responsibilities, for all third-party personnel.

b) Require providers of third-party personnel to comply with personnel security policies and procedures established by the Collaboratory.
c) Document personnel security requirements
d) Require third party providers to notify Collaboratory human resources of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system, or within a period of 5 business days.
e) Monitor provider compliance.

[PS-8] PERSONNEL SANCTIONS

Collaboratory Human Resources, in cooperation with system managers, will document a process, compliant will all Federal, state, local and contractual legal requirements, to apply formal sanctions.

a) Collaboratory's sanction process will be employed against individuals who fail to comply with established information security policies and procedures.
b) The process will notify affected supervisors and personnel when sanctions proceedings begin that a formal sanctions process has been initiated, identifying the individual sanctioned and the reason for the sanction.

RISK ASSESSMENT

[RA-1] RISK ASSESSMENT POLICY AND PROCEDURES

Collaboratory will maintain policies and procedures governing risk assessment.

a) Risk assessment policies and procedures will be distributed to all Security Assessors, Developers, System Managers, System Owners, Incident Response Managers, Security, and executives within the Collaboratory.

b) All Risk Assessment Policies and Procedures must undergo periodic review, such that

1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.

2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle

[RA-2] SECURITY CATEGORIZATION

The System Owner role is responsible for the categorization of all information systems and data within the Collaboratory.

a) Categorization must occur in accordance with all Federal, state, local and contractual legal requirements.
b) Security plans will be updated to document the security categorization results and supporting rationale for information systems and data.
c) Authorizing officials (or designees) must approve the security categorization decision(s).

[RA-3] RISK ASSESSMENT

Modern information security and risk assessment is premised on being able to clearly identify and delineate authorization boundaries, which must be documented in security plans. Risk assessment considers threats, vulnerabilities, likelihood and impact to organizational System Owner and assets, individuals, and other organizations based on the operation and use of information systems. Risk assessment also takes into account risk from external parties (e.g. service providers, contractors, outsourcing entities, and individuals accessing organizational information systems), as well as public access risk to information systems. Note that risk assessment is a precursor to successful implementation of this policy framework. Toward this end, Collaboratory will:

a) Conduct an assessment of risk, including the likelihood and magnitude of harm, resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores and transmits.
b) Document, in Collaboratory security planning documents, the risk assessment results.
c) Review risk assessment prior to any changes being made to the system and at least once every 15 months, with an intended one-year cadence.

d) Disseminate risk assessment results to Developers, System Managers, Delivery and Experience, Security and the Executive.
e) Update the risk assessment as part of the security plan reviews, prior to making configuration or system changes, as part of the lessons learned phase of incident response, and whenever new vulnerability and threat information about an information system becomes known.

[RA-5] VULNERABILITY SCANNING

Vulnerability scanning includes activities that identify potential and actual techniques, methods, and attackable surfaces affecting information systems. Vulnerability scanning is an intelligence function, that helps to inform system managers and developers, influence work priorities and resourcing decisions, and feeds the risk assessment function to help identify the probability and impact of security events. Collaboratory will:

a) Scan for vulnerabilities on its information at least as often as recommended by product vendors and integrators, or in the absence of vendor guidance once per quarter. A full schedule of routine scanning activities (including system update/patch checks, configuration checks, unauthorized change, and log monitoring) will be maintained covering each system manager, which should be reviewed and approved by System Owner and Security.
b) Utilize, to the extent practical with available resources, vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact.
c) Analyze the results of vulnerability scan reports and results from security control assessments.
d) Remediate legitimate vulnerabilities as quickly as possible, in accordance with an organizational assessment of risk; and
e) Share information obtained from the vulnerability scanning process and security control assessments with System Managers, Developers, System Owners, and Security to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

[ENHANCED] [RA-5 (1)] UPDATE TOOL CAPABILITY

Collaboratory will select and employ vulnerability scanning tools, including malware protection, that include the capability to readily update the information system vulnerabilities to be scanned.

[ENHANCED] [RA-5 (2)] UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED

Collaboratory will update the information system vulnerabilities scanned prior to new scans to ensure that the most current vulnerabilities are scanned for.

[ENHANCED] [RA-5 (5)] PRIVILEGED ACCESS

Systems performing automated vulnerability scanning will be jointly authorized by System Owner and Security to perform those scans prior to use. Scanning of systems will be authorized by the System Owner (or higher in that owner's reporting chain) of scanned systems.

SYSTEM AND SERVICES ACQUISITION

[SA-1] SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Collaboratory will maintain policies and procedures governing system and service acquisition.

a) System and service acquisition policies and procedures will be distributed to all procurement roles, including relevant subsets to any individual requesting or approving information system procurement decisions within the Collaboratory.

b) All Risk Assessment Policies and Procedures must undergo periodic review, such that

1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.

2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle.

[SA-2] ALLOCATION OF RESOURCES

In any organization, resources are allocated commensurate with commitment levels to the extent they are available. To facilitate informing management and resource allocation priorities:

a) Information security requirements will be determined for all information systems and information system services as part of the mission/business planning process.
b) Resources required to protect the information system or service will be determined, documented, and allocated as part of the Collaboratory's capital planning and investment control process.
c) Information security will have a discrete line item in organizational budget documents.

[SA-3] SYSTEM DEVELOPMENT LIFE CYCLE

A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To facilitate a more secure system development life cycle, Collaboratory will:

a) Adopt or document a full system development life cycle that incorporates information security considerations;
b) Define and document information security roles and responsibilities throughout the system development life cycle;
c) Identify individuals having information security roles and responsibilities; and
d) Integrate the organizational information security risk management process into system development life cycle activities.

[SA-4] ACQUISITION PROCESS

Collaboratory will include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable Federal, state, local and contractual legal requirements to meet business needs:

a) Security functional requirements;
b) Security strength requirements;
c) Security assurance requirements;
d) Security-related documentation requirements;
e) Requirements for protecting security-related documentation;
f) Description of the information system development environment and environment in which the system is intended to operate; and
g) Acceptance criteria.

[ENHANCED] [SA-4 (1)] FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

Collaboratory information system and service developers must provide a description of the functional properties of the security controls to be employed on those systems.

[ENHANCED] [SA-4 (2)] DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS

Collaboratory requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces; and high-level design in sufficient detail to allow for risk assessment by System Owners assisted by security personnel.

[ENHANCED] [SA-4 (9)] FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE

Developers of information systems, system components, and information system services must identify and document early in the system development life cycle any functions, ports, protocols and services intended for organizational use.

[SA-5] INFORMATION SYSTEM DOCUMENTATION

Modern information systems, especially those built on general purpose computing devices, are remarkably complex and frequently require the ability to reference specific details about the operation and use of the equipment and software. The lack of timely access to needed documentation can impact operations, security or service delivery and can occur, for example, due to the age of the information system/component or lack of support from developers and contractors. As such, Collaboratory will curate documentation associated with its information systems, including the procurement, generation, maintenance, archiving and protection of documentation of its information systems in accordance with system criticality and risk.

Toward this end, Collaboratory will:

a) Obtain administrator documentation for the information system, system component, or information system service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service;
    2. Effective use and maintenance of security functions/mechanisms; and
    3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b) Obtain user documentation for the information system, system component, or information system service that describes:
    1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
    2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
    3. User responsibilities in maintaining the security of the system, component, or service;
c) Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and mitigate the risks associated with missing documentation by either generating those documents or strategically accelerating the lifecycle of such information systems and components to removing improperly documented components to lead to such systems being replaced by more modern, properly documented alternative functionalities;
d) Protect documentation as required, in accordance with the risk management strategy; and
e) Distribute documentation on a need-to-know basis to system managers, developers and security evaluation personnel, or in accordance with a documented and authorized business need to users or other personnel.

Third-party software often has widely available Internet-based documentation that remains available for substantial periods of time, either through subscription, registration, or at no charge. For purposes of this policy, documentation which remains available via the Internet is considered “obtained” if finding the documentation is detailed in Collaboratory-maintained documents and any necessary access accounts are maintained. However, the risk that Internet-based documentation would become unavailable—especially software approaching end-of-support, end-of-life, or supported by a company facing acquisition or at risk of terminating operation—must be considered per (d) above in accordance with an organizational risk management strategy.

[ENHANCED] [SA-8] SECURITY ENGINEERING PRINCIPLES

Collaboratory will apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system. Primarily, this applies to new development and major upgrades; however, legacy systems will be retrofitted through upgrades and modifications to the extent feasible given the current state of hardware, software and firmware within those systems. Security engineering principles include, but are not limited to:

- Developing layered protections;
- Establishing sound security policy, architecture, and controls as the foundation for design;
- Incorporating security requirements into the system development life cycle;
- Delineating physical and logical security boundaries;
- Ensuring that system developers are trained on how to build secure software;
- Tailoring security controls to meet organizational and operational needs;
- Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and
- Mitigating risk to acceptable levels, thus enabling informed risk management decisions.

[SA-9] EXTERNAL INFORMATION SYSTEM SERVICES

External information system services are services that are implemented outside of the authorization boundaries of Collaboratory information systems. The reliance on external service providers does not inherently satisfy Collaboratory's security requirements: external information systems that process, store or transmit information on behalf of the Collaboratory are required to meet or exceed the security requirements for internally operated systems. The responsibility for managing these risks – whether through joint ventures, business partnerships, interagency agreements, contracts, line-of-business arrangements, licensing agreements, or any other relationship with an external service provider – still remains with the authorizing official. To set expectations on performance for security controls, describe measurable outcomes, identify remedies and identify response requirements for potential noncompliance, Collaboratory will utilize service level-driven agreements that:

a) Require providers of external information system services to comply with organizational information security requirements and employ all applicable policy-defined controls;
b) Define and document Collaboratory's oversight and user roles and responsibilities with regard to external information system services; and
c) Define and employ appropriate processes, methods and techniques to monitor security control compliance by external service providers on an ongoing basis.

[ENHANCED] [SA-9 (2)] IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES

External service providers must identify functions, ports, protocols and services used in the provision of the various features of the external service prior to authorization to facilitate the trade-offs associated with restricting certain functions or attempting to enforce controls within Collaboratory systems.

[ENHANCED] [SA-10] DEVELOPER CONFIGURATION MANAGEMENT

The quality and completeness of the configuration management activities conducted by developers is taken as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized

changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on business needs and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle.

Toward that end, Collaboratory requires the developer of the information system, system component, or information system service to:

a) Perform configuration management during the design, development, and implementation of the system, component, or service
b) Document, manage, and control the integrity of changes to configuration, components, and software source code (or object code, if the software is not customized or internally developed);
c) Implement only organization-approved changes to the system, component, or service;
d) Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e) Track security flaws and flaw resolution within the system, component, or service and report findings to the system manager and security incident response manager.

[ENHANCED] [SA-11] DEVELOPER SECURITY TESTING AND EVALUATION

Developmental security testing/evaluation must occur at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws.

Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor (e.g. black box, grey box, white box) to be applied, and the types of artifacts produced during those processes. The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. To meet these ends,

Collaboratory requires the developer of the information system, system component, or information system service to:

a) Create and implement a security assessment plan;
b) Perform unit, integration, system and regression testing/evaluation in using existing expected use and predicted abuse cases whenever substantive system changes occur;
c) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d) Implement a verifiable flaw remediation process; and
e) Correct flaws identified during security testing/evaluation.

SYSTEM AND COMMUNICATIONS PROTECTION

[SC-1] SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Collaboratory will maintain policies and procedures governing system and communication protection.

a) System and communication protection procedures will be distributed to System Managers, Security Assessors and Developers. Further, training specific to any role required to execute any procedure related to system and communication protection will be included for all relevant roles within the Collaboratory.

b) All System and communication protection Policies and Procedures must undergo periodic review, such that

1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.

2. Procedures will always undergo a documentation review and reconciliation process every 15 months, with a preferred 1-year cycle.

[ENHANCED] [SC-2] APPLICATION PARTITIONING

All information systems separate user functionality (including user interface services) from information system management functionality.

[ENHANCED] [SC-4] INFORMATION IN SHARED RESOURCES

All information systems prevent unauthorized and unintended information transfer via shared system resources.

[SC-5] DENIAL OF SERVICE PROTECTION

Information systems protect against or limit the effects of the select types of denial of service attacks. Specific classes of attacks will be identified and specific countermeasures will be established to safeguard information systems. Denial of service attacks can originate from external or internal sources. Information system resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Common safeguards to prevent denial of service attacks related to storage utilization and capacity include, for example, instituting disk quotas, configuring information systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data. Within virtualized, aggregated, and multi-tenant environments, separation will consider both the physical as well as logical segmentation. In-application limitations may also be imposed.

[SC-5 (1)] RESTRICT INTERNAL USERS

Countermeasures above will be utilized to restrict the ability of individuals to launch denial of service attacks across administrative control zones, including internal users. Process segmentation at the

operating system level, or session segmentation within the application, will be used to minimize the impact of denial of service attacks within administrative control zones.

[SC-5 (2)] EXCESS CAPACITY / BANDWIDTH / REDUNDANCY

Information systems will manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.

[SC-5 (3)] DETECTION / MONITORING

Collaboratory will consider utilization and capacity of information system resources when managing risk from denial of service due to malicious attacks. Toward that end, Collaboratory will:

a) Establish and employ monitoring tools to detect indicators of denial of service attacks against the information system; and
b) Monitor the levels of CPU, memory, disk/storage, and network bandwidth utilization to determine if sufficient resources exist to prevent effective denial of service attacks.

[SC-7] BOUNDARY PROTECTION

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. To enforce boundary protection and help establish boundaries between administrative control zones, Collaboratory will:

a) Monitor and control communications at the external boundary of the system and at key internal boundaries within the system;
b) Implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and
c) Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

[ENHANCED] [SC-7 (3)] ACCESS POINTS

Collaboratory will limit the number of external network connections to the information system.

[ENHANCED] [SC-7 (4)] EXTERNAL TELECOMMUNICATIONS SERVICES

Collaboratory will manage external telecommunications services to:

a) Implement a managed interface for each external telecommunication service;
b) Establish a traffic flow policy for each managed interface;
c) Protect the confidentiality and integrity of the information being transmitted across each interface;
d) Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
e) Review exceptions to the traffic flow policy at least once every 15 months with an intended 1-year cadence, and removes exceptions that are no longer supported by an explicit mission/business need.

[ENHANCED] [SC-7 (5)] DENY BY DEFAULT / ALLOW BY EXCEPTION

All managed telecommunications interfaces will deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

[ENHANCED] [SC-7 (7)] PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

Information systems that allow access to a remote device will, in conjunction with the remote device, prevents the device from simultaneously establishing non-remote connection with the system and communicating via some other connection to resources in external networks.

[ENHANCED] [SC-8] TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Transmission of data which leaves the administrative control zone from which it originates is potentially exposed to the possibility of modification or interception. Both technical and procedural methods will be utilized to protect both confidentiality and integrity of transmitted information. Specific techniques will be established and approved for use within specific risk profiles and information classifications such the use of encryption.

[ENHANCED] [SC-8 (1)] CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION

The information system implements cryptographic mechanisms to prevent unauthorized disclosure or modification of information during transmission unless otherwise protected by approved physical safeguards.

[SC-10] NETWORK DISCONNECT

The information system terminates the network connection associated with a communications session at the end of the session or after 5 minutes of inactivity.

[SC-12] CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Collaboratory will document procedures for cryptographic key management in accordance with current technologies in use. Procedures will minimally address acceptable methods for key generation, minimum protection measures to ensure secure distribution, storage, access, and destruction of cryptographic keys. All procedures will be drafted to meet the following objectives in accordance with the level of risk associated with the applications the keys will be used for:

a) Prevent disclosure of private and symmetric keys to unauthorized users, uses, and applications.

b) Protect private and public keying data from damage or corruption.
c) Ensure necessary keys are available when needed for tasks required in support of Collaboratory functions.

Absent other guidance, system cryptographic keys will be generated on a secure, offline system maintained for the purpose generating cryptographic keys. Keys will be manually transferred via physical data media (such as a USB thumb drive or read-only media such as CD-R) to the destination system by trusted Collaboratory personnel. Physical data media will be maintained in a physically secure location when not in use. Keys, once installed, will be kept on the intended system–using every reasonably available system measure to protect private key and symmetric key data that does not undermine the intended purpose. Expired and rotated away keys will be promptly removed from online systems but retained on secure, offline media until reasonable assurance can be obtained that the keys are no longer required.

[SC-13] CRYPTOGRAPHIC PROTECTION

The information system implements all encryption in accordance with applicable Federal, state, local and contractual legal requirements. Collaboratory will utilize the guidance from NIST's Federal Information Processing Standards FIPS Publication 140-2 or its successor(s) for cryptographic implementations.

[SC-15] COLLABORATIVE COMPUTING DEVICES

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated. All information systems within the Collaboratory will:

a) Prohibit remote activation of collaborative computing devices unless an exception (with associated risk assessment) is authorized; and
b) Provide an explicit indication of use to users physically present at the devices.

[ENHANCED] [SC-17] PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Collaboratory will only issue public key certificates from an approved service provider or, if self-issued, based on an approved and authorized organization defined certificate policy in the framework format defined by the Internet Engineering Task Force in document RFC3647 (http://www.ietf.rfc/rfc3647.txt) or (if obsoleted) an RFC or standards-track successor Internet standard.

[ENHANCED] [SC-18] MOBILE CODE

Collaboratory systems will not utilize mobile code technologies (e.g. Java, JavaScript, ActiveX, PostScript, PDF, Shockwave movies, Flash animations, or VBscript) and such technologies will be by default disabled on all Collaboratory systems unless and until the Collaboratory:

a) Defines acceptable and unacceptable mobile code and mobile code technologies;

b) Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies;
c) Authorizes, monitors, and controls the use of mobile code within the information system.

[ENHANCED] [SC-19] VOICE OVER INTERNET PROTOCOL

Collaboratory will address Internet telephony and Voice over Internet Protocol technologies by:

a) Establishing usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
b) Authorizing, monitoring, and controlling the use of VoIP within the information system.

[SC-20] SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

The information system:

a) Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
b) Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

[SC-21] SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

[SC-22] ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

[ENHANCED] [SC-23] SESSION AUTHENTICITY

The information system protects the authenticity of communications sessions.

[ENHANCED] [SC-28] PROTECTION OF INFORMATION AT REST

The information system protects confidentiality of all non-public information at rest.

[SC-39] PROCESS ISOLATION

The information system maintains a separate execution domain for each executing process.

SYSTEM AND INFORMATION INTEGRITY

[SI-1] SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Collaboratory will maintain policies and procedures governing system and information integrity.

a) System and information integrity procedures will be distributed to system managers, security assessors and developers. Further, any role expected to execute any procedure related to system and communication protection will be required to undertake training applicable to that role within the Collaboratory.
b) All System and information integrity Policies and Procedures must undergo periodic review, such that:
    1. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.
    2. Policies will always have undergone a review/approval cycle within 39 months (3 years, 3 months), with a preferred 3-year cycle.

[SI-2] FLAW REMEDIATION

As a matter of policy and process, Collaboratory will:

a) Identify, report, and correct information system flaws;
b) Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c) Install security-relevant software and firmware updates within two weeks of the release of the updates unless contraindicated based on testing; and
d) Incorporate flaw remediation into the organizational configuration management process.

[ENHANCED] [SI-2 (2)] AUTOMATED FLAW REMEDIATION STATUS

Absent other documented and approved guidance, Collaboratory will employ automated mechanisms on at least a daily basis to determine the state of information system components with regard to flaw remediation.

[SI-3] MALICIOUS CODE PROTECTION

To facilitate the protection of information systems and data from exploitation by adversaries, Collaboratory will:

a) Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b) Update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c) Configure malicious code protection mechanisms to:
    1. Perform periodic scans of the information system weekly and real-time scans of files from external sources at endpoints (with the permissible but not required augmentation

of real-time scanning at entry and exit points as technology is implemented) as the files are downloaded, opened, or executed in accordance with organizational security policy; and

2. Quarantine or block malicious code in response to malicious code detection; and

d) Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

[ENHANCED] [SI-3 (1)] CENTRAL MANAGEMENT

Collaboratory will centrally manage malicious code protection mechanisms.

[ENHANCED] [SI-3 (2)] AUTOMATIC UPDATES

Collaboratory information systems will be configured to automatically update malicious code protection mechanisms.

[SI-4] INFORMATION SYSTEM MONITORING

Collaboratory will remain situationally aware of its information systems both from an internal and external standpoint, such that it:

a) Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives; and
   2. Unauthorized local, network, and remote connections;
b) Identifies unauthorized use of the information system through audit logs and anomaly detection;
c) Deploys monitoring devices:
   1. Strategically within the information system to collect organization-determined essential information; and
   2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable Federal, state, local and contractual legal requirements; and
g) Provides access regarding specific systems to their system managers, and all information to internal and external security assessors and incident response managers or any other Collaboratory or external personnel as authorized and needed.

[ENHANCED] [SI-4 (2)] AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

Collaboratory will employ automated tools to support near real-time analysis of events.

[ENHANCED] [SI-4 (4)] INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

The information system monitors inbound and outbound communications traffic on a daily basis for unusual or unauthorized activities or conditions.

[ENHANCED] [SI-4 (5)] SYSTEM-GENERATED ALERTS

The information system alerts system managers and incident response managers upon detection of any approved indicators of compromise or potential compromise. Collaboratory will establish and document an appropriate set of compromise indicators based on the functions performed by its information system resources.

[SI-5] SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government and makes that information available to the public. Vendors also typically include security communications and alerts. To facilitate information system situation awareness, Collaboratory will:

a) Receive information system security alerts, advisories, and directives from US-CERT, external information owners, and vendor incident response teams on an ongoing basis;
b) Generate internal security alerts, advisories, and directives as deemed necessary;
c) Disseminate security alerts, advisories, and directives to system managers and developers; and
d) Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

[ENHANCED] [SI-7] SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Collaboratory will employ integrity verification tools to detect unauthorized changes to approved software, firmware, and system configurations.

[ENHANCED] [SI-7 (1)] INTEGRITY CHECKS

The information system performs an integrity check of software, firmware, and system configuration at the time of deployment/documented update, and on an ongoing basis to occur at least a quarterly.

[ENHANCED] [SI-7 (2)] AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS

The information system performs an integrity check of software, firmware, and system configuration on an automated schedule in accordance with a risk/criticality assessment.

[ENHANCED] [SI-7 (7)] INTEGRATION OF DETECTION AND RESPONSE

Collaboratory will incorporates the detection of unauthorized changes to software, firmware, and configuration into its incident response capability.

[ENHANCED] [SI-8] SPAM PROTECTION

Collaboratory will take action to minimize the impact of unsolicited junk email ("spam") and will:

a) Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b) Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

[ENHANCED] [SI-8 (1)] CENTRAL MANAGEMENT

Collaboratory will centrally manage spam protection mechanisms.

[ENHANCED] [SI-8 (2)] AUTOMATIC UPDATES

Collaboratory information systems will automatically update spam protection mechanisms.

[ENHANCED] [SI-10] INFORMATION INPUT VALIDATION

All information system code developed by Collaboratory will implement secure coding techniques which must check the valid syntax and semantics of user- and externally provided information system inputs (e.g., character set, length, numerical range, and acceptable values); and verify that inputs match specified definitions for format and content.

[ENHANCED] [SI-11] ERROR HANDLING

Collaboratory developers and system integrators will carefully consider the structure/content of error messages and must not include information that could be exploited by adversaries. Because error conditions can and often do occur when dealing with sensitive information, care will be taken to avoid exposing, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers.

The information system:

a) Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
b) In cases where detailed error data may expose sensitive data, error messages will be revealed only to authorized personnel (System Managers, support personnel and Developers working on fault identification/resolution).

[SI-12] INFORMATION HANDLING AND RETENTION

Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems.

Collaboratory will handle and retain information within its information systems and information output from its system in accordance with operational requirements and conform to all applicable Federal, state, local and contractual legal requirements.

[ENHANCED] [SI-16] MEMORY PROTECTION

Barring other guidance, all Collaboratory-developed information systems will implement data execution prevention and utilize secure coding specific to the underlying operating-system provided security features to protect its memory from unauthorized code execution.