(AMSM)

2016 System Security Plan

Version 4.0

February 24, 2017

Sensitive But Unclassified (SBU)

DOCUMENT REVISION HISTORY

Date	Version	Description	Author
05/27/2016	1.0	Document Published	Kristi Gilliat, NORC
10/26/2016	2.0	Updated based on CDC Feedback	Kristi Gilliat, NORC
11/08/2016	3.0	Updated based on CDC Feedback	Kristi Gilliat, NORC
02/24/2017	4.0	Updated based on CDC Feedback	Kristi Gilliat, NORC

DOCUMENT APPROVALS

______________________________	__________
{fullname}	Date
AMSM Program Manager	
______________________________	__________
{full name}	Date
AMSM Business Steward	
______________________________	__________
{fullname}	Date
AMSM Information System Security Officer	

Table of Contents

1.0 SYSTEM CHARACTERIZATION

1.1 System Name and Unique Project Identifier (Exhibit 300 and/or Exhibit 53)

The system name is Adolescent Men Having Sex with Men Study (AMSM). The Enterprise Systems Catalog (ESC) System ID is xxxx.

1.2 System Type

Adolescent Men Having Sex with Men Study is a General Support System.

1.3 System Categorization

Adolescent Men Having Sex with Men Study has been categorized as [insert risk level – assumption was Moderate when completing this document].

1.4 System Status

Adolescent Men Having Sex with Men Study is New Development.

1.5 Responsible Organization

1.6 Information POC

The following is contact information for Adolescent Men Having Sex with Men Study System Stewards and Designated Approving Authority (DAA).

1.6.1 Points of Contact

Table 2: Points of Contact

Name	
Office Symbol	Centers for Disease Control and Prevention
Title	Certification Agent
Organization	
Address	
Telephone	
Email	
Responsibility	Certification Agent

Name	
Office Symbol	Centers for Disease Control and Prevention
Title	DAA
Organization	
Address	

Telephone	
Email	
Responsibility	CDC Designated Authorization Agent (DAA)

Name	Ralph Vaughn
Office Symbol	Centers for Disease Control and Prevention
Title	ISSO
Organization	Department of Health and Human Services
Address	CORP Bldg 8 Rm 6079 MS E08 Atlanta, GA 30329-1902
Telephone	404.639.1806
Email	rxv2@cdc.gov
Responsibility	CDC Information System Security Office (ISSO)

Name	
Office Symbol	Centers for Disease Control and Prevention
Title	Business Steward
Organization	
Address	
Telephone	
Email	
Responsibility	CDC Business Steward Responsibility

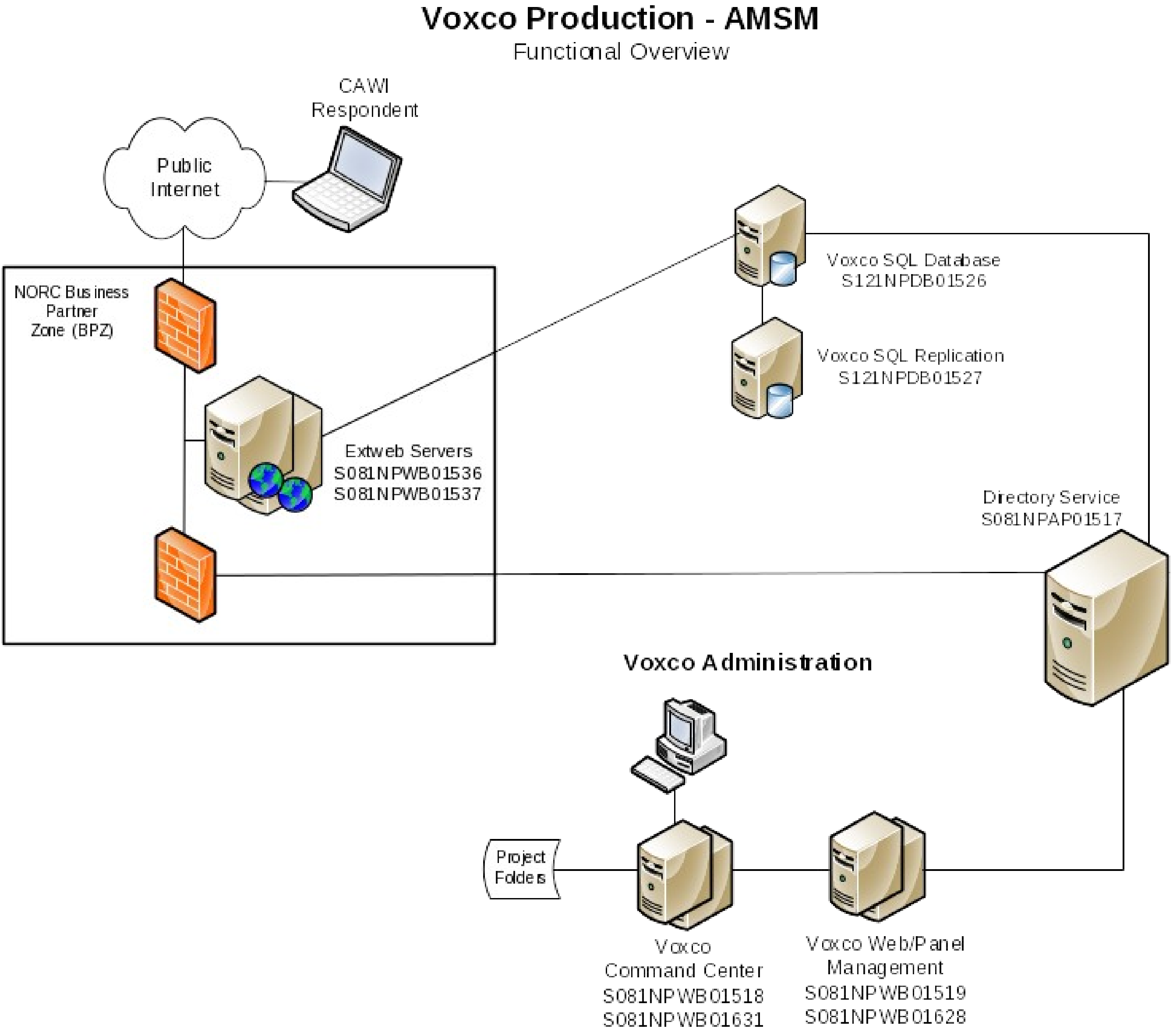
Name	
Office Symbol	Centers for Disease Control and Prevention
Title	Security Steward
Organization	
Address	
Telephone	
Email	
Responsibility	CDC Security Steward Responsibility

1.7 General Description / Purpose

During year one of the projected three year study, NORC will develop and pilot test a web-based survey of Adolescent Men Having Sex with Men (AMSM) ages 13 to 18 with input from subject matter experts and a youth advisory board. A social media recruitment strategy will also be developed in partnership with Socially Authentic, a social media consulting firm. In year two, the survey will be administered to a national sample of AMSM using social media platforms for recruitment (e.g., Facebook, Kik, etc.), while focus groups are conducted to supplement the survey data. The final year involves data analysis to help translate findings into tools and guidance for public health practitioners, develop and field a social media based recruitment plan and survey instrument to collect data from adolescent MSM 13 to 18 years old, with over-sampling of Black and Latino MSM to inform prevention efforts and produce evidence-based tools and guidance that work in this population. The survey will include topics related to sexual identity, behavior, HIV risk protective factors, and acceptability of HIV prevention strategies. To test the survey, cognitive testing will be conducted with 9 individuals who mirror the study population of 13-18 year olds, with an emphasis on Blacks and Latinos (as they experience a higher prevalence of HIV). We will also pilot the survey via web utilizing technology-based strategies for recruitment with adolescents who were born male who are attracted to or have sex with males.

There are major gaps in evidence-based prevention tools to target adolescent MSM and engage them in new, innovative HIV prevention efforts. This innovative research project aims to better understand the unique characteristics and behaviors of this specific demographic in order to develop tools and guidance to better inform them of HIV prevention strategies.

1.8 System Environment



1.9 System Interconnection / Information Sharing

Table 3: System Interconnection/Information Sharing

System Name	Organization	Type (TCP/IP, Dial-up, SNA, etc.)	Agreement (ISA/ MOU/ MOA/SLA)	Date of Agreement	Security Categorization	Authorization Status	Name and Title of Authorizing Official
No interconnections defined.							

1.9.1 System Dependencies

Beyond these dependencies, a set of common dependencies was defined to enable boundary definition. A dependency is a telecommunication or information technology interconnection or resource on which the system under review relies for processing, transport, or storage. The relationship between the system in question and the dependencies can directly affect the confidentiality, integrity, or availability of the system or its data. Whenever a system has a dependency, the system inherits the intrinsic risks of the dependent asset. The following Centers for Disease Control and Prevention (CDC) information technology resources can be considered dependencies:

- CDC Enterprise Policies
- CDC Enterprise Application Hosting Branch
- CDC Network Infrastructures:
    - Center or Information Technology Services Office (ITSO) Local Area Networks
    - Atlanta Metropolitan Area Network
    - CDC Wide Area Network
    - Internet Connectivity
- DMZ Connectivity
- CDC Enterprise Security Services:
    - CDC Border Firewall
    - CDC Border Router Access Control Lists
    - Network-Based Intrusion Detection Systems
    - E-Mail Gateway Protection-Virus Scanning and Attachment Removal
    - RSA SecurID Authentication System
- Technical Vulnerability Scanning Service (Most Commonly Used for Hosts Deployed to the DMZ)
- CDC Computer Room Staff, Physical, and Environmental Controls
- CDC Exchange Services:
    - Enterprise E-Mail Gateway Infrastructure with Gateway Protection
    - ITSO or Center Managed Local E-Mail Stores with Server Virus Protection
    - Remote Access Web Mail Services with RSA SecurID Authentication
- CDC Enterprise Continuity of Operations and Disaster Recovery Planning
- CDC Enterprise Windows Domain/Active Directory Environment

1.9.2 Supported Programs and Applications

1.10 Applicable Laws or Regulations Affecting the System

As an operating division of the U.S. Department of Health and Human Services (DHHS), CDC is responsible for implementing and administering a program to protect its information resources in compliance with federal laws and regulations. The following denotes applicable laws and regulations, standards, and guidelines from which DHHS and CDC system security requirements are derived.

Executive Orders (EO)

- EO 10450 Security Requirements for Government Employment
- EO 12958 Classified National Security Information
- EO 12968 Access to Classified Information
- EO 10310 Critical Infrastructure Protection
- EO 13011 Federal Information Technology
- EO 13103 Computer Software Piracy
- Homeland Security Presidential Directive 7

Federal Laws

- Title II of the E-Government Act of 2002, Section 208
- Privacy Act of 1974 (P.L. 93-579)
- Freedom of Information Act of 1974
- Federal Records Management Acts
- Computer Fraud and Abuse Act of 1986 (P.L. 99-474)
- Clinger-Cohen Act of 1996
- Defense Authorization Act (P.L. 106-398)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L. 104-191)
- Federal Information Security Management Act of 2002 (FISMA)

National Institute of Standards and Technology (NIST) Special Publication (SP) and Guidelines

- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-16, Information Technology Security Training Requirements
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30, Risk Management Guide for Information Technology Systems
- NIST SP 800-34, Contingency Planning Guide for IT Systems
- NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-44, Version 2, Guidelines on Securing Public Web Servers
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems
- NIST SP 800-60 Revision 1, Vol. 1 & 2, Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-63, Electronic Authentication Guideline: Recommendation of the National Institute of Standards and Technology
- NIST SP 70, The NIST Security Configuration Checklists Program
- NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling
- NIST SP 800-86, Guide to Integrating Forensic Techniques Into Incident Response
- NIST SP 800-92, Guide for Computer Security Log Management
- NIST SP 800-95, Guide for Secure Web Services
- NIST SP 800-97, Guide to IEEE 802.111: Establishing Robust Security Networks (this is related to wireless network deployment)

Federal Information Processing Standards Publications (FIPS)

- FIPS PUB 140-2, Security Requirements for Cryptographic Modules
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors

Office of Management and Budget (OMB) Circulars and Government Accounting Office (GAO) Requirements

- OMB Circular No. A-130, Appendix III
- OMB Circular No. A-123, Management Accountability and Control
- OMB Memorandum 99-18, Privacy Policies on Federal Web Sites
- OMB M 99-20, Security of Federal Automated Information Resources
- OMB M 00-07, Incorporating and Funding Security in Information Systems Investments
- OMB M-13, Privacy Policies and Data Collection on Federal Web Sites
- OMB M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB M-04-04, E-Authentication Guidance for Federal Agencies
- Federal Information System Controls Audit Manual (FISCAM)

DHHS and CDC Institutional Rules and Guidance

- Department of Health and Human Services Information Security Program Policy, December 15, 2004
- Department of Health and Human Services Information Technology (IT) Privacy Impact Assessment (PIA) Guide, July 12, 2004
- Information Resources Management CDC-3
- DHHS 45 CFR Part 142, Security and Digital Signature Standards
- DHHS 45 CFR 164.500, Privacy Requirement Exemptions

1.11 FIPS 199 Levels

FIPS 199 establishes three potential impact levels (Low, Moderate, High) for each of the security objectives (confidentiality, integrity, and availability). The impact levels focus on the potential impact and magnitude of harm that the loss of confidentiality, integrity, or availability (C/I/A) would have on CDC's operations, assets, or individuals. FIPS 199 recognizes that an information system may contain more than one type of information (e.g., privacy information, medical information, financial information), each of which is subject to security categorization.

The following table provides the definitions for C/I/A ratings for AMSM Study.

Table 4: Security Objectives

Security Objective	Low	Moderate	High
Confidentiality **Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 USC, SEC. 3542]**	**The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**	**The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.**	**The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.**

Security Objective	Low	Moderate	High
Integrity **Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 USC, SEC. 3542]**	**The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**	**The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.**	**The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.**
Availability **Ensuring timely and reliable access to and use of information. [44 USC, SEC. 3542]**	**The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.**	**The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.**	**The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.**

1.11.1 Security Categorization/Information Type(s)

The security category of an information system that processes, stores, or transmits multiple types of information should be at least the highest impact level that has been determined for each type of information for each security objective of C/I/A. The following table depicts the security category/information type for **Adolescent Men Having Sex with Men Study** as identified in the AMSM Study Risk Assessment Report.

Table 5: AMSM Study Information Type

Name	Information Category	Information Type	Confidentiality	Integrity	Availability	Justification
C.2.1.3 Controls and Oversight: Program Monitoring	Controls and Oversight	Program Monitoring	Moderate	Moderate	Low	
CIA Overall Security Categorization:			Moderate	Moderate	Low	
System Security Categorization:						Moderate

Note: If C/I/A ratings differ from NIST SP 800-60, provide justification and obtain approval from the Office of the Chief Information Security Officer (OCISO).

1.11.2 Protection Requirements

Both information and information systems have distinct life cycles. It is important that the degree of sensitivity of information be assessed by considering the requirements for the C/I/A of the information: the need for system data to be kept confidential; the need for the data processed by the system to be accurate, and the need for the system to be available. Confidentiality focuses on the impact of disclosure of system data to unauthorized personnel. Integrity addresses the impact that could be expected should system data be modified or destroyed. Availability relates to the impact to the organization should use of the system be denied.

1.11.3 Protection Requirement Findings

- **Confidentiality:** [*Example:* **AMSM Study** *contains sensitive information that could identify a survey participant. This data requires protection from unauthorized disclosure. If information contained in* **AMSM Study** *were released to the public it could result in a loss of public confidence in the survey, affect participation, and cause a great deal of embarrassment to the CDC*]. Therefore, the unauthorized disclosure of **AMSM Study** information could be expected to have a (**limited, serious, or severe**) adverse effect on organizational operations, organizational assets, or individuals and the information and protection measures are rated as **(Low, Moderate, High)**.
- **Integrity:** [*Example:* **AMSM Study** *collects and processes health and nutritional information annually from a representative sample of the U. S. population. Because public health trends and policies depend on the accuracy of the data collected, unauthorized and unanticipated modification would seriously reduce the accuracy of the survey results*]. Therefore, the unauthorized modification of **AMSM Study** information could be expected to have a (**limited, serious, or severe**) adverse effect on organizational operations, organizational assets, or individuals and the information and protection measures are rated as **(Low, Moderate, High)**.
- **Availability:** [*Example: If* **AMSM Study** *were unavailable for even a short period of time, it would have an immediate impact and would affect the efficiency with which* **AMSM Study** *typically operates*]. Therefore, the unavailability of **AMSM Study** information could be expected to have a (**limited, serious, or severe**) adverse effect on organizational operations, organizational assets, or individuals and the information and protection measures are rated as **(Low, Moderate, High)**.

Note: Security Controls and Security Control Enhancements in Sections 2, 3, and 4 MUST be addressed. If a control does not apply to the system enter N/A with justification.

1.12 System Host Matrix

Table 6: System Host Matrix

Name	IP Address	Subnet	IP Range	Vendor	Product	Model	Version	Hostname	Port	Protocol	Supported Modules	Patch Level	Location	Description

2.0 MANAGEMENT CONTROLS

2.1 (CA) Security Assessment and Authorization

2.1.1 CA-1 Security Assessment and Authorization Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Assessment and Authorization Policy” which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Security Assessment and Authorization
The NORC Security Assessment and Authorization Procedures contains documented procedures to facilitate the implementation of the systems and services policy and associated controls. This document is located under the CA-1 security control.
NORC reviews organization-wide policies and procedures annually, which NORC defines as within every 365 days. If any changes are made, NORC policy and procedures are adjusted accordingly.

2.1.2 CA-2 Security Assessments, including Enhancement CA-2(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:

The NORC project-specific system Security Assessment Plan(s) define the controls requiring assessment. Security self-assessment tools and templates are provided by each agency requesting the execution of the assessment. The assessment is typically executed by the IT Security Compliance Supervisor under the guidance of the ISO Director. The assessment includes interviews with key ISO, TSS and business Stakeholder personnel, observation of system and operations processing, observation of technical and physical security controls, collection of evidence supporting security controls claims, review of security scans, identification of remediation items, and documentation of all findings.

NORC conducts an assessment of security controls annually and conducts an external assessment of all security controls every three years to determine the extent to which the controls are implemented correctly and operating as intended. Additionally, weekly active host vulnerability and compliance scanning, weekly asset discovery scanning, continuous real-time passive vulnerability scanning, monthly open port scanning is performed. A security assessment report is provided which details summary and specific findings. The security assessment report is provided to the Project Directors, agency, senior management, and all others responsible for ensuring project continuation and success, which may include the funding of remediation and compliance activities.

NORC conducts both independent assessments and security self-assessments. An independent assessment uses an external assessor with a strong understanding of NIST 800-53 Rev. 4 standards to verify that the controls are in place and working properly with the objective of proving compliance.

2.1.3 CA-3 System Interconnections, including Enhancement CA-3(5)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC currently has no dedicated connections to any information systems outside the authorized boundary for the AMSM study. Therefore this control is not applicable at this time. Should NORC require connections from information systems within the NORC authorization boundary in the future, NORC will carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within NORC and external to NORC.

If interconnections between NORC systems and external systems are made, NORC authorizes such connections via an Interconnection Security Agreement (ISA) or other acceptable documentation that identifies for each connection, the interface characteristics, security requirements, and the nature of the information communicated. Additionally, NORC monitors those information system connections on an ongoing basis and verify that security mechanisms are functioning properly, and adequately enforcing required security controls relative to connections to external information systems.

2.1.4 CA-5 Plan of Action and Milestones

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC, in coordination with the CDC assigned Security Steward, develops plan of action and milestones (POA&M) for its Agency information systems to provide a medium in which system security weaknesses or deficiencies are 1) reported to proper authorities and; 2) tracked until resolution is achieved. POA&Ms are updated quarterly in accordance the respective regulatory agency guidance. Each quarter, the agency reviews and comments on all POA&Ms to ensure all necessary issues are addressed properly.

2.1.5 CA-6 Security Authorization

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Regardless of whether the security authorization responsibility is for Federal Agency systems or NORC-specific systems, a senior level executive is assigned to act as the authorizing official for every project's information system(s). For Federal Agency systems, security authorization is an inherently federal responsibility and therefore, authorizing officials must be federal employees. For NORC systems that do not process or store federal agency data, security authorization for systems is a function of the NORC Chief Information Officer (CIO) in conjunction with input from the respective NORC IT Directors and favorable security assessment completed by the NORC Information Security Officer (ISO).

This individual authorizes the information system for processing before commencing operations. This individual also updates the security authorization on a periodic basis per requirements relative to system operation. Federal systems require reaccreditation every three years or when a major change to the system occurs. Systems may require a security reauthorization if the risks to the information systems change significantly.

2.1.6 CA-7 Continuous Monitoring, including Enhancement CA-7(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
A continuous monitoring program allows NORC to maintain the security authorization of its information systems over time in lights of ever-changing threats, vulnerabilities, technologies, and missions and/or business processes.
A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities at NORC are scaled in accordance with the security categorization of the information system

NORC IT - Continuous Monitoring strategy
NORC establishes a continuous monitoring strategy and implements a continuous monitoring of its IT assets. NORC's continuous monitoring strategy consists of the following characteristics:
- A Configuration Management (CM) process for the information system and its constituent components.
- Weekly CM meeting are held by the IT Engineering Team to prioritize and report status of configuration management issues that includes system installation, integration, and maintenance activities, such as patching systems.
- Security Impact Analyses (SIA) of changes to the information system and environment of operation, and the resulting determination of the analyses in accordance with NORC IT-121 Security Impact Analysis. This reference is located under the CM-4 security control.
- IT Engineering staff conducts an SIA when new hardware or software will be introduced to the system or changes to existing resources are made to provide assurance that the system will not incur and adverse security impact.
- Ongoing security control assessments.
- Part of proper CM and continuous monitoring is providing ongoing assessments of security controls. NORC constantly assesses its security posture against existing security controls against risks and threats to the system via it automated monitoring tools. NORC also re-evaluates its security controls when new security controls and/or guidelines are introduced by NIST CSRC or any changes to existing controls are made.
- Monthly reporting of the security state of the information systems to appropriate NORC Management, CDC System Owner and CDC ISSO.

Current status of NORC systems is conveyed by IT Engineering Team Members at weekly CM Meetings. The IT Engineering Director and ISO then provide input and feedback on the security status of NORC systems to the CIO and Agency officials, as appropriate.

Continuous Monitoring Automated Tools
Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system.
The four primary, automated tools used by NORC for continuous monitoring include:

- eIQ SecureVue situational awareness suite
- Nessus' Tenable Security Center; and
- Shavlik NetChk Protect patch management software
- Zayo's ERP monitors entry into data center facilities and physical and environmental controls

2.1.7 CA-9 Internal System Connections

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
a. The ISO Network Engineering Team, under the guidance of the ISO Director (CISO) is accountable for managing internal connections between geographic subnets and network zones on a least-privilege basis. Connections are typically authorized for information system components by type classification (i.e., mobile devices, desktops and laptops, output devices). Some classification types (i.e., servers) carry out specialized functions, in which connections are established at a more granular level. All connections are opened by TCP port and protocol to allow defined types of traffic, which are dependent on business need.
b. Documentation includes an overall network architecture, detailed network segment diagrams, data flow diagrams, Security Impact Analyses, Change Control records, and descriptions (definitions) of network zones.

2.2 (PL) Planning

2.2.1 PL-1 Security Planning Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC Security, Security Planning Policy, is the formal, documented security planning policy and addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities/personnel (i.e., the system administrators, ISSOs, system owners/business owner, and users etc.), and compliance. This reference is located under the PL-1 security control.

The NORC Security, Security Planning Procedures, contains documented procedures to facilitate the implementation of the Security Planning policy and associated Security Planning controls. This reference is located under the PL-1 security control.

Continuous Monitoring – NORC reviews organization-wide policies and procedures annually, which NORC defines as every 365 days. If any changes are made, NORC policy and procedures are adjusted accordingly.

2.2.2 PL-2 System Security Plan, including Enhancement PL-2(3)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC develops all of its SSPs in accordance with NIST SP 800-53 Revision 4, which states that system security plans for its information systems meet the following conditions:

- Consistent with NORC's infrastructure architecture
- Defines the authorization boundary for the system
- Describes the operational information system in terms of mission and business processes
- Provides the security categorization of the information system Describes the operational environment for the information system
- Describes the relationships with or connections to other information systems
- Provides an overview of the security requirements for the system
- Describes the security controls in place or planned for meeting those requirements including supplemental decisions
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation

NORC system security plans are reviewed on an annual basis, defined by NORC as every 365 days. The plan is updated as necessary to address changes to the information system and environment of operation or problems identified during plan implementation or security control assessments.

The NORC IT Security Compliance Manager maintains a master System Security Plan, which documents the information security profile and plan for the organization as a whole. Security plans are maintained in a secure file storage environment and are encrypted with password protection.

NORC coordinates any project and/or client-specific security related activities affecting the information systems with the project owner, agency and other affected parties prior to conducting activities to reduce the impact of the activities.

2.2.3 PL-4 Rules of Behavior, including Enhancement PL-4(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:

The NORC Rules of Behavior (RoB) delineates the responsibilities and expected behavior of all individuals with access to NORC information systems.

Individual Federal agency projects on which NORC performs work also have their own Rules of Behavior. NORC employees' who work on those projects must sign the related Project RoB form prior to performing work on the project.

Rules of behavior documentation is reviewed at least every three years and updated as changes are needed. Rules of Behavior that have had changes made must be re-signed by all affected employees.

NORC's rules of behavior address the use of social media/networking sites and restrict the posting of organization information on any public website. If applicable, Individual Federal agency projects on which NORC performs work, specifies restrictions for social media and public website use.

2.2.4 PL-8 Information Security Architecture

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:

The NORC secure information systems environment has been designed to ensure the functions and protection of data controls meet the confidentiality, integrity and availability standards associates with the NIST 800-53 framework.

The NORC ISO Team maintains enterprise and information security architecture and information systems configuration documentation in accordance with NORC's evolving security profile to reflect current business functionality and regulatory requirements. The team consults with the Senior Contract Administrator (Chief Privacy Officer) when engaging with external partners to ensure that strong information security and privacy controls extend beyond NORC network domain.

NORC reviews and updates the security architecture on no less than an annual basis to reflect updates in enterprise architecture and privacy requirements.

Key documents include: System Security Plans, Configuration Management Plan, System Authorization Boundary documents, network and system architecture diagrams and supporting documentation. All of these documents contain a Concept of Operations statement. The architectural philosophy is a key driver of procurement/acquisition decisions.

2.3 (RA) Risk Assessment

2.3.1 RA-1 Risk Assessment Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC Security, Risk Assessment Policy, is the formal, documented risk assessment policy and addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This reference is located under the RA-1 security control. The NORC Security, Risk Assessment Procedures, contains documented procedures to facilitate the

implementation of the risk assessment policy and associated risk assessment controls. This reference is located under the RA-1 security control.
Continuous Monitoring – NORC reviews organization-wide policies and procedures annually as defined within every 365 Days. If any changes are made, NORC policy and procedures are adjusted accordingly.

2.3.2 RA-2 Security Categorization

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC uses methodologies established in FIPS 199 for performing security categorization with guidance from NIST SP 800-30, 800-39 and 800-60 to ensure systems are categorized in compliance accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance.

NORC documents security categorization results including supporting rationale in the security plan for the information system.

The security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

2.3.3 RA-3 Risk Assessment

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Risk Assessments are conducted annually to determine the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of this information system.

A risk assessment report provides documentation of the risk assessment activities and results.

Risk assessment results are disseminated to the IT Senior Management Team, including the CIO (Authorizing Official).

Risk Assessments are updated at least every three years or whenever there are significant changes to the information system that impact the accreditation status of the system.

2.3.4 RA-5 Vulnerability Scanning, including Enhancements RA-5(1) (2) (5)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC scans for system vulnerabilities in its information systems on a weekly basis, and when new vulnerabilities potentially affecting the system/application are identified and reported.

NORC employs a vulnerability scanning tool that promotes interoperability between tools and automates parts of the vulnerability process by using standards for Enumerating platforms, software flaws, and improper configurations, Formatting and making transparent, checklists and test procedures, and Measuring vulnerability impact. The vulnerability scanner also has the capability to readily update the list of information system vulnerabilities scanned. To accomplish vulnerability scanning, NORC uses Tenable Security Center and NESSUS v5.02 (or greater) is to be used to perform vulnerability scans. NESSUS uses the following standards, information repositories, and methodologies to generate and maintain a database of vulnerabilities.

NORC analyzes vulnerability scan reports and results from security control assessments. Following a scan, findings can be reviewed using the Security Center reporting module or exported and reviewed offline. The NESSUS scanners categorize findings by severity.

NORC remediates legitimate vulnerabilities in various timeframes in accordance with an organizational assessment of risk. If a fix exists it must be tested and implemented within two patching cycles (maximum four weeks). Any vulnerability deemed to be an immediate and serious risk must be addressed within 48 hours.

NORC also shares information obtained from the vulnerability scanning process and security control assessments with designated personnel within NORC's ISO Department and with our customers, as necessary, to help eliminate similar vulnerabilities in other information systems.

The Nessus vulnerability scanner has been configured to update the list of information system vulnerabilities to be scanned. NORC maintains a subscription to Tenable Nessus Plugins Feed to get daily updates of known vulnerabilities. The vulnerability scanner updates its vulnerability database prior to a new scan.

NORC has implemented privileged access authorization for ISO Engineers to operating systems, databases and web applications for all scans. This limits the ability for non-privileged users to access scanning tools and modify scanning settings.

Monthly reporting of the security state of the information systems to appropriate NORC Management, CDC System Owner and CDC ISSO.

2.4 System and Services Acquisition (SA) Controls

2.4.1 SA-1 System and Services Acquisition Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC Security, Systems and Services Acquisition Policy, is the formal, documented systems and services policy and addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

The NORC Security, Systems and Services Acquisition Procedures, contains documented procedures to facilitate the implementation of the systems and services acquisition policy and associated system and services acquisition controls.

Continuous Monitoring – Both the NORC-wide and project policies and procedures are updated annually, defined by NORC as every 365 days.

2.4.2 SA-2 Allocation of Resources

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC Information Technology department includes a determination of information security requirements for its information systems in mission and business process planning.

The NORC Deputy Director of Finance for IT within the Office of the CIO manages the annual and projected budgets for the NORC IT department as part of its capital planning and investment control process.

The NORC IT capital planning and investment control process determines, documents, and allocates the resources required to protect NORC information systems and includes discrete line items for information security in NORC IT programming and budgeting documentation.

2.4.3 SA-3 System Development Life Cycle

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The life cycle methodology and processes utilized by the NORC Information Technology Department follow the linear, sequential, Waterfall model, with modifications, as appropriate. The Agile method is implemented if deemed appropriate.

NIST Special Publication 800-64 defines the Systems Development Life Cycle (SDLC) with the following phases as shown in Figure.1:
- Initiation: The need for a system is expressed and the purpose of the system is documented.
- Development/Acquisition: The system is designed, purchased, programmed, developed, or otherwise constructed.
- Implementation/Assessment: The system is tested, and once accepted, is installed or fielded.
- Operation/Maintenance: The system is in production and performs its work but is almost always

modified by the addition of hardware and software or by numerous other events.
• Disposal: The system disposition is closed out. Orderly termination of the system is performed while ensuring the safeguarding of vital system information and migrating any data processed by the system to a new system, or preserving it in accordance with applicable records management regulations and policies.

Information Security roles and their respective responsibilities are defined for each phase or each of the life cycle models used. In many cases, several of the same roles have responsibilities within each phase of the life cycle model used, but the degree of those responsibilities in those roles may be more or less intensive depending on the phase. Roles defined are: System Owner, ISO, Change Control Board members, Configuration Manager, Administrators and Engineers, Database Administrators and Engineers, Acceptance Testers, and Auditors.

NORC identifies individuals having information system security roles and responsibilities. The individual(s) associated with a role are defined in the applicable control family policy documents.

2.4.4 SA-4 Acquisition Process, including Enhancement SA-4(1) (2) (9) (10)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC includes the relative security functional, strength, assurance, documentation requirements and/or specifications in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Additionally, NORC includes the requirements protecting security-related documentation requirements and/or specifications in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

NORC ensures that a description of requirements for a secure system development environment are defined in systems and services acquisition documents, in which the system is intended to operate.

NORC ensures that acceptance criteria to ensure successful implementation of functional and security requirements are directly or indirectly referred via attachment or exhibit, within systems and services acquisition contracts.

NORC 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; design and implementation information describing the functional properties of the security controls to be employed within the information system in sufficient detail to permit analysis and testing of the controls.

The developer is required to explicitly define the required ports, protocols and services needed for use, during the design phase.

Since NORC in not a federal agency, NORC is also not able accept and electronically verify Personal Identity Verification (PIV) credentials from federal agencies. All implemented products must be FIPS compliant.

No CDC users will be accessing the AMSM system; only survey participants.

2.4.6 SA-5 Information System Documentation

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:

Administrator documentation
Administrator documentation addresses secure configuration, installation and operation of the information system. It also covers effective use and maintenance of security features and functions as well as known vulnerabilities regarding configuration and use of administrative functions. NORC Administrator documentation primarily consists of vendor documentation regarding setup, security configuration, software permissions but also includes third party information to supplement the vendor documentation. This documentation contains sufficient detail to permit analysis and testing of the security controls associated with the system component or service. The documentation also describes the high level design of the system in terms of subsystems and implementation of security controls.

NORC also provides end-user documentation that describes user accessible security features and functions as well as how to effectively use those functions. It also describes methods for user interaction with the information system to enable users the ability to use the system(s) in a more secure manner. Lastly, the end-user documentation espouses user’s responsibilities in maintaining security of both the information and the information system(s).

NORC documents attempts to obtain information system documentation when the documentation is unavailable or non-existent and creates Incident or Change documentation in Footprints helpdesk tickets to create the documentation in response.

NORC maintains a local repository for quick internal access to critical documentation. This also ensures access to the documentation in case of loss of access to the documentation source.

IT Security Policies are distributed to Senior IT Management, Project Directors, and Privacy Program personnel. IT Security Procedures are available for the NORC IT teams on the secure LANADM shared drive.

2.4.7 SA-8 Security Engineering Principles

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC applies information system security engineering principles in the specification, design, development, implementation, and modification its information systems and software applications. Security Engineering principles must be applied in accordance with, and supplement, the controls and principles associated with NORC’s Enterprise and Information Security Architecture, which are documented in NORC SOP, IT-46 (PL-8 & PM-7 & AR-7) - Enterprise & Information Security Architecture.

NORC develops layered protections and deploys those safeguards throughout the NORC IT Infrastructure using Defense-in-Depth strategies.

NORC establishes sound security policies, system architecture, and security controls when designing systems and software. NORC references a numerous Federal Government policies early in the Life Cycle to pinpoint areas for compliance. CIS Benchmarks, USGCB and FDCC are all utilized to ensure there is a timely, verifiable and repeatable way of securing NORC hardware and software assets that are part of the NORC systems architecture.

NORC references NIST Special Publication 800-27 for information system security engineering principle guidelines. These principals are integrated into the Life Cycle Models used by NORC IT.

2.4.8 SA-9 External Information System Services, including Enhancement SA-9(2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
This security control is not applicable to the AMSM system as there are no external information system services connections outside the system boundary.

2.4.9 SA-10 Developer Configuration Management

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Developer and Integrator Configuration Management (CM) at NORC take place throughout the Life Cycle. NORC Application Development (APPDEV) uses two Life Cycle Models for application development: the Software Development Lifecycle (SDLC) and the Agile Development Model. Configuration Management activities, like information security activities, take place during, design, development, implementation and operation.

Changes related to NORC software development come in the form of Change Requests which can originate from any of the project stakeholders within NORC. Other changes come in the form of requirements documentation usually originating from the ITPS Business Analyses Team. Some projects are created to make changes to a system.
NORC Application Developers use Subversion versioning software to manage version changes to software.
NORC software developers are responsible for documenting changes to the software. Changes can also be documented by Business Analyses in the requirements documentation or directly via Technical Support Services via a Footprints Ticket for smaller changes.

Changes are submitted by any of the project stakeholders within NORC and approved by project management team. Once changes are approved the requirements for the change are forwarded to development team.

Changes are tracked throughout the Life cycle by every Team. AppDev uses Subversion versioning software to track their code changes. NORC’s APPDEV Software Developers are responsible for integrity of the code the write and are for reviewing code prior to submission. These code reviews include nominal checks for the most obvious software vulnerabilities and flaws such as those included within the OWASP Top Ten Web Application Vulnerabilities as well as the SANS/MITRE Top 25 Software Flaws. Software security flaws, once discovered are tracked in Subversion until resolved.

NORC currently uses Nessus for tracking security flaws and flaw resolution within the system.

2.4.10 SA-11 Developer Security Testing

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has multiple methods to ensure web applications contain code that is as secure as possible. One way this is accomplished is to conduct automated security scans of the code. Another way is to conduct a security peer review of the code as part of the development lifecycle.

NORC conducts unit, integration, system and regression testing/evaluation in accordance with the OWASP testing guide.

Documenting the results of the security testing/evaluation and flaw remediation processes is done via the JIRA Issue Tracking application. Also, if applicable, completed Flaw Remediation form(s) will be attached to the JIRA ticket.

NORC tracks flaws through to remediation in Jira. The details of the flaw are outlined and assigned to a developer for remediation. Upon remediation, the ticket is updated to contain details of the remediation in the JIRA ticket. A Quality Assurance engineer verifies the flaw is completely remediated.

2.5 Program Management (PM) Controls

2.5.1 PM-1 Information Security Program Plan

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Information Security Program Policy” which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Security Assessment and Authorization.

NORC has developed and maintains a series of Information Security Program procedures, reflective of the controls required by the NIST 800-53 standard, and which define the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Security Assessment and Authorization. The policy and procedures are distributed to IT Management, Senior Management and Project Directors.

The CDC Enterprise:

NIST Requirement a.

All CDC policy and procedure documents are disseminated as indicated in the descriptions below to allow access to each document for system administrators, ISSOs, system owners/business owners, and other users defined by the system owner.

HHS has developed the policy *HHS-OCIO Policy for Information Systems Security and Privacy* (HHS-OCIO-2014-0001). HHS-OCIO-2014-0001 establishes comprehensive IT security and privacy requirements for the IT security programs and information systems of OPDIVs and STAFFDIVs. The policy can be found on the HHS Intranet.

The *HHS-OCIO Information Systems Security and Privacy Policy Control Section* (i.e., aka Control Section) outlines IT security and privacy policy requirements for IT security and privacy programs and information systems in more detail, and is organized according to Information Assurance (IA) control families to make the document easy to use and scalable for the future. HHS requires all OPDIVs to implement security in relation to Program Management (PM) in compliance with the current revision of NIST SP 800-53. HHS policy guidance on the implementation of (PM) can be found in the Handbook. The Handbook can be found on the HHS Intranet.

CDC has published the policy referred to as the *Protection of Information Resources* (CDC-IS-2002-06). CDC-IS-2002-06 establishes policy for the protection of Centers for Disease Control and Prevention (CDC) data, information, and information technology systems; thereby protecting and enhancing the reputation, image, legal position, and other tangible and intangible assets of CDC. The policy can be found on the CDC Intranet.

The CDC-IS-2002-06, states “operational standards for implementing federal laws, OMB, National Institute of Science and Technology (NIST), HHS and CDC policies and guidance concerning protection of IT resources will be delineated in the *CDC IT Security Program Implementation Standards*” which can be found on the CDC Intranet. CDC guidance on Program Management (PM) is provided in the *CDC IT Security Program Implementation Standards.*

NOTE: In the case of both the HHS handbook and the *CDC IT Security Program Implementation Standards*, these documents can serve as both policy and procedures implementation documents for HHS and/or the CDC.

The CDC has developed and published the policy *In- and Out- Processing of CDC Employees, Non-Employees, and Affiliates* (CDC-GA-2007-01) and the link to this policy can be found on the CDC Intranet.

CDC-GA-2007-01 establishes the *In- and Out-Processing* which encompasses the entire lifecycle of logical (i.e., electronic or computer-based) and physical access to information and resources required by someone working at or associated with CDC.

HHS-OCIO-2014-0001 addresses purpose, scope, roles and responsibilities. The HHS policy is formally approved by the HHS Chief Information Officer (CIO) showing management commitment to required information security policy, including formal authorization. Furthermore, HHS-OCIO-2014-0001 addresses coordination throughout the policy. This policy, and its complimentary handbook, lay out the compliance for HHS Information Systems Security.

CDC-IS-2002-06 addresses purpose, scope, responsibilities. The CDC policy is formally approved by the CDC Chief Information Officer (CIO) showing management commitment to required information security policy, including formal authorization. Furthermore, CDC-IS-2002-06 has implemented the *CDC IT Security Program Implementation Standards* which addresses purpose, scope, management commitment, coordination, and compliance. The standard also includes the adoption of HHS Information Security policy. This policy, and its complimentary standard, lay out the compliance for CDC Information Systems Security.

CDC-GA-2007-01 addresses purpose, scope, responsibilities. The CDC policy is formally approved by the CDC Chief Information Officer (CIO). CDC-GA-2007-01 has implemented the *CDC IT Security Program Implementation Standards* which addresses purpose, scope, management commitment and compliance in the document. This standard is formally approved by the CDC Chief Information Security Officer (CISO). Furthermore, this standard also addresses coordination throughout the document. This policy, and its complimentary standard, lay out the compliance for CDC Information Systems Security.

All HHS policies link to HHS Office of the Chief Information Officer (OCIO) Policies, Standards and Charters page on the HHS Internet, which serves as the authoritative source for all HHS OCIO policies. The OCIO policies can be found on the HHS Intranet.

CDC Management Policy, such as CDC-IS-2002-06, is disseminated by the Management Analysis and Services Office (MASO) via the CDC Intranet and can be found on the CDC Intranet.

Office of the Chief Information Security Officer (OCISO) standards and policy are distributed on the OCISO website located on the CDC Intranet.

All links to the policy websites are the CDC Intranet, available to all CDC authorized users, including those with Program Management (PM) roles. Announcements of policy updates are made through CDC Today – Daily Announcements distributed to all CDC personnel (federal and contractors) via CDC Mail. OCISO maintains email distribution lists to more directly contact IT security personnel (i.e., ISSOs and Stewards) concerning policy changes for information security.

OCISO maintains email distribution lists to more directly contact IT security personnel (i.e., ISSOs and Stewards) concerning policy changes for information security

In- and Out- Processing of CDC Employees, Non-Employees, and Affiliates (CDC-GA-2007-01) are disseminated by the Management Analysis and Services Office (MASO) via the CDC Intranet and can be found on the CDC Intranet.

OCISO reviews/updates policies and procedures on an annual basis in accordance with the annually published Cyber Security Action Plan which can be located on the CDC Intranet.

NIST Requirement b.

All CDC policy and procedure documents are reviewed and updated on an annual basis

CDC-IS-2002-06, specifically states that operational standards for implementing federal laws, OMB, National Institute of Science and Technology (NIST), HHS, and CDC policies and guidance concerning protection of IT resources are delineated in the *CDC IT Security Program Implementation Standards*. CDC guidance on Program Management (PM) is provided in the *CDC IT Security Program Implementation Standards* which can be found on the CDC Intranet.

CDC-GA-2007-01 specifically states that operational standards for implementing federal laws, OMB, National Institute of Science and Technology (NIST), HHS and CDC policies and guidance concerning protection of IT resources will be delineated in the *CDC IT Security Program Implementation Standards* on the CDC Intranet. CDC guidance on Program Management (PM) is provided in the *CDC IT Security Program Implementation Standards*.

The *CDC IT Security Program Implementation Standards* specifies and explains the Centers for Disease Control and Prevention (CDC) Information Technology (IT) security program requirements and minimum mandatory standards for the implementation of information security and privacy within CDC. It incorporates by reference the requirements of Public Laws, Federal and Departmental [i.e., Office of Management and Budget (OMB), Department of Health and Human Services (HHS)] regulations, IT Security Laws and Federal Regulations, along with CDC policies, procedures, standards, and guidelines. This document also supports implementation of the Information Security Program Plan controls in compliance with the current revision of NIST SP 800-53.

Per the CDC procedures defined in *In- and Out- Processing of CDC Employees, Non-Employees and Affiliates* (CDC-GA-2007-01) ITSO procedures are dependent upon OSEP and MISO policy and procedures to define and grant access to cleared personnel within the CDC. CDC Active Directory provides additional granularity for the C/I/O’s at the program level.

OCISO standards and policies can be found on the CDC Intranet.

All links to the policy websites are the CDC Intranet, available to all CDC authorized users, including those with Program Management (PM) roles. Announcements of policy updates are made through CDC Today – Daily Announcements distributed via CDC Mail. OCISO maintains email distribution lists to more directly contact IT security personnel (i.e., ISSOs and Stewards) concerning policy changes for information security.

CDC C\I\O’s disperses formal documented Program Management (PM) procedures to their personnel that have associated Program Management (PM) roles and responsibilities.

OCISO reviews/updates policies and procedures on an annual basis in accordance with the annually published Cyber Security Action Plan which can be located on the CDC Intranet.

2.5.2 PM-2 Senior Information Security Officer

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has appointed a Senior Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

The CDC Enterprise:

CDC's CIO appoints, in writing, a senior information security officer (i.e., CDC's CISO) to coordinate, develop, implement, and maintain an organization-wide information security program.

2.5.3 PM-3 Information Security Resources

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC ensures that all capital planning and investment requests include the resources needed to implement the information security program.

NORC employs a business case to record the resources required.

NORC ensures that information security resources are available for expenditure as planned.

The CDC Enterprise:

NIST Requirement a.

Not Applicable (N/A). The individual capital planning and investment requests no longer include the resources needed to implement the information security program. The resources needed to implement the information security program are now captured at the agency level on the OMB Exhibit 53B, "Agency IT Security Portfolio."
A link to OMB Guidance on Exhibits 53 and 300 can be found in the CDC IT Security Program Implementation Standards.

The resources typically identified on the OMB Exhibit 53B are:

- Agency Code
- Number of government Full Time Equivalents (FTEs) with information security responsibilities
- Average cost per government FTE with information security responsibilities
- Number of contractor FTEs with information security responsibilities
- Average cost per contractor FTE for information security responsibilities
- Total IT security tools cost
- Costs for NIST 800-37 implementation
- Number of systems scheduled for activities represented in Row 7 (Costs for NIST SP 800-37 implementation)
- Costs for annual FISMA testing
- Costs for network penetration testing activities
- Security awareness training costs
- Security training costs for employees with significant security responsibilities
- Number of government FTEs included in costs for row 7 and rows 9 through 12
- Number of contractor FTEs included in costs for row 7 and rows 9 through 12

No formal exception process exists, however, CDC is required to report the resources needed to implement the information security program at the agency level each year on the OMB Exhibit 53B.

NIST Requirement b.

Major IT investments no longer report a discrete line item for information security on the OMB Exhibit 300. The OMB Exhibit 53A no longer includes a discrete line item for information security. The OMB Exhibit 53B, does establish a discrete line item for total IT security costs at the agency level.
Office of the Chief Information Security Officer (OCISO) is responsible for identifying the information security resources required (at the agency level) and for completing the OMB Exhibit 53B (at the agency level).

NIST Requirement c.

Not Applicable (N/A). There is no direct correlation between the planned fiscal year information security resources reported on the OMB Exhibit 53B, and the final information security resources expenditure made available to agency organizational components during the respective fiscal year.

2.5.4 PM-4 Plan of Action and Milestones Process

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.

NORC documents its development, implementation, and updating of NORC information system POA&Ms.

The CDC Enterprise:

NIST Requirement a.

OCISO has developed and implemented a process to maintain Plan of Action and Milestones (POA&M) which is part of a larger SA&A process. The SA&A process is part of the agency's security program and is the driving force behind how information systems are authorized. The security program can be referenced in the *CDC IT Security Program Implementation Standards*.

As part of the SA&A process, findings from security control assessments, security impact analyses, and continuous monitoring activities are captured in an information system or enterprise POA&M. The Certification Agent reviews POA&M items, negotiates an acceptable period of time allotted to correct each milestone, and signs the POA&M to demonstrate their approval. OCISO developed and also maintains the *OCISO POA&M Tracking & Reporting Standard Operating Procedure* (SOP) which outlines roles and responsibilities and POA&M reporting requirements. A link to this document can be found in the *CDC IT Security Program Implementation Standards*.

Additionally, Trusted Agent is a CDC-wide tool that is currently used to track weaknesses and associated information tied to those weaknesses for all information systems within the agency.

OCISO has developed and implemented the POA&M process to document the remedial information security actions that mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

OCISO reports POA&M items to HHS every quarter of the fiscal year.

NIST Requirement b.

As part of the SA&A processes that create enterprise POA&M items, CDC reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

2.5.5 PM-5 Information System Inventory

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC develops and maintains an inventory of its information systems. For those that require it, an inventory of all information system components is maintained.

This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.

The CDC Enterprise:

OCISO has developed the OCISO inventory which tracks all information systems within CDC. OCISO's Inventory Coordinator is responsible for maintaining the OCISO Inventory inside the OCISO Trusted Agent system. The following items are tracked and updated within the inventory:

- System name
- Acronym
- ESC ID
- Organization
- Program
- Division
- ISSO
- Business steward
- DAA
- EMSSP or Full
- Internal or External
- In development or in production
- EMSSP joined
- ATO date
- ATO expiration
- SA Completion date
- BCP completion date
- Late or Near due dates for ATO, SA, or BCP
- E-Auth level
- Access indication
- Critical indication
- Reportable inventory
- Reportable system
- SSN

If there are any changes to the aforementioned items, then the Inventory Coordinator is responsible for updating the inventory. Additionally, the Inventory Coordinator submits two reports each week for the ISSOs to verify the information contained within the report. A new inventory record is created daily in case it's necessary to go back or recreate the inventory. These records are kept in a folder on the link-share which is a shared drive available to only authorized OCISO personnel.

2.5.6 PM-6 Information Security Measures of Performance

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:

NORC develops, monitors, and reports on the results of information security measures of performance.

Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

- NORC develops metrics that allow for monitoring of the performance of NORC information systems and measure the effectiveness of specific security controls.
- The results of this monitoring are available to the NORC Engineering Team and NORC ISSO.
- NORC incorporates the results into its information security program

The CDC Enterprise:

The appendices of the yearly Cyber Security Action Plan (CSP), include projected milestone tasks. Under each task, there is a timeframe in which that task must be completed. Time is used as a measure of performance. A link to the CSP can be found in the in the CDC IT Security Program Implementation Standards.

There are three teams (i.e., Privacy, Policy & Planning, and Operations) within OCISO that monitor and report on the results of information security measures (i.e., time) of performance.

For the Privacy team, the Chief Privacy Officer ensures that the tasks are completed per the timetables found in the CSP. Also, the Chief Privacy Officer completes the tasks and reports progress to the Privacy Specialist. The Privacy Specialist then notifies the CISO's Administrative Assistant who updates the CSP tracking chart accordingly.

For the Policy and Planning team, the Policy and Planning Management and Program Analyst ensure that the personnel are meeting the tasks per the timetables found in the CSP. Also, as personnel complete a task, they notify the Policy and Planning Management and Program Analyst who submits the report of progress to the Policy and Planning ACISO. The Policy and Planning Management and Program Analyst then notify the CISO's Administrative Assistant who updates the CSP tracking chart accordingly.

For the Operations team, the Operations Management and Program Analyst ensure that the personnel are meeting the tasks per the timetables found in the CSP. Also, as personnel complete a task, they notify the Operations Management and Program Analyst who notifies the Operations ACISO. The Operations Management and Program Analyst then update the CSP tracking chart accordingly.

2.5.7 PM-7 Enterprise Architecture

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC secure information systems environment has been designed to ensure the functions and protection of data controls meet the confidentiality, integrity and availability standards associates with the NIST 800-53 framework. The NORC ISO Team maintains enterprise and information security architecture and information systems configuration documentation in accordance with NORC’s evolving security profile to reflect current business functionality and regulatory requirements. The team consults with the Senior Contract Administrator (Chief Privacy Officer) when engaging with external partners to ensure that strong information security and privacy controls extend beyond

NORC network domain.
Key documents include: System Security Plans, Configuration Management Plan, System Authorization Boundary documents, network and system architecture diagrams and supporting documentation.

For further details, please see NORC SOP IT-46, Enterprise & Information Security Architecture.

The CDC Enterprise:

HHS, in coordination with the CDC, develops an enterprise architecture (EA) with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. HHS requires security and privacy practices to protect information assets from unauthorized use, disclosure, disruption, modification, or destruction. A link to the *CDC EA Reference Guide*, which describes the CDC EA program, can be found in the *CDC IT Security Program Implementation Standards*.

2.5.8 PM-8 Critical Infrastructure Plan

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

The CDC Enterprise:

Critical infrastructure and key resource protection is defined and described within the Continuity of Operations (COOP) Plan – Centers for Disease Control and Prevention. This document is developed and maintained by OSSAM, OCISO, ITSO, MISO, and the various centers, institutes and offices (C/I/Os) who 'own' the critical systems identified within these documents. Although access to the COOP documents is controlled by OSSAM, a copy of the documents may be provided for viewing, if needed.

2.5.9 PM-9 Risk Management Strategy

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems and implements that strategy consistently across the organization.

NORC incorporates acceptable risk assessment methodologies, risk mitigation strategies, and monitoring risk into its organizational risk management strategy. NORC accomplishes this by using guidance from NIST 800-30 and by implementing security controls defined in NIST 800-53 based on the information system's security classification.

The risk management strategy is updated as necessary, to address organizational changes.

The CDC Enterprise:

NIST Requirement a.

OCISO develops a comprehensive risk management strategy in the *Cyber Security Action Plan* (CSP) to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems. A link to this document can be found in the in the *CDC IT Security Program Implementation Standards.*

NIST Requirement b.

OCISO implements the comprehensive risk management strategy consistently across the organization by updating it as defined by the organization and posting it to the CDC Intranet.

NIST Requirement c.

OCISO review and updates a comprehensive risk management strategy as described in *CDC IT Security Program Implementation Standards, APPENDIX K: CDC IT Security Organizationally-Defined Minimum Numbers and Time Periods.*

2.5.10 PM-10 Security Authorization Process

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes, designates individuals to fulfill specific roles and responsibilities within the organizational risk management process, and fully integrates the security authorization processes into an organization-wide risk management program.

- NORC documents, tracks and reports this state through the Plan of Action and Milestones documented in NORC SOPs relative to Security Assessment and Authorization as well as any System Security Plan for specific systems.
- NORC designates individuals to fulfill these roles and responsibilities throughout NORC's information security documentation.
- NORC's integration of the security authorization process is fully documented in the NORC Security Assessment and Authorization Policies and Procedures.

The CDC Enterprise:

NIST Requirement a.

OCISO manages (i.e., documents, tracks, and reports) the security state of CDC information systems through security authorization processes. OCISO utilizes an inventory to track information systems and the different areas tied to those systems. Refer to PM-5 for the details on how the inventory is maintained and reported on, also Trusted Agent is used as a repository for system documentation. The application also has tracking and auditing mechanisms.

NIST Requirement b.

OCISO designates individuals to fulfill specific roles and responsibilities within the organizational risk management process. Designated staff includes ISSO's, security stewards, the SA&A team, and Security Operations personnel. Management roles include the CISO, DCISO, and two ACISOs. The DAA has designated other DAAs at an information system level to accept risks for systems.

NIST Requirement c.

CDC fully integrates the security authorization processes into an organization-wide risk management program. The CDC Enterprise Architecture (EA) Program includes the CDC Enterprise Project Lifecycle (EPLC). One of the phases of EPLC, the Implementation Phase, contains the system Security Assessment and Authorization project reviews which encompass the first five steps of the Risk Management Framework. The link to the CDC EA Reference Guide, which describes the program, can be found in CDC IT Security Program Implementation Standards.

The CDC Continuous Monitoring Implementation Plan describes the approach for implementation of the automated continuous monitoring capabilities at CDC.
S081NPWB01519
The CDC Continuous Monitoring Implementation Plan establishes the procedures for the automated continuous monitoring of CDC IT system security controls against those documented and approved during the associated SA&A process. These procedures encompass the last step of the Risk Management Framework.

The link to the CDC Continuous Monitoring Implementation Plan guidance document can be found in the CDC IT Security Program Implementation Standards.

2.5.11 PM-11 Mission / Business Process Definition

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation and determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

- NORC information systems which are determined to have information protection needs must follow the security processes defined in NIST 800-53 for the information system’s security categorization.
- Information protection needs are taken into account during the information system’s security categorization process, which determines the required security controls and processes needed to support the mission/business processes.

The CDC Enterprise:

NIST Requirement a.

The Office of Safety, Security, and Asset Management (OSSAM)identifies critical infrastructure required to support the CDC mission/business needs and works with the various programs throughout CDC to develop the procedures necessary to protect those assets and key resources.

OCISO is the proponent for the CDC Protection of Information Resources policy, which establishes the policy for the protection of CDC data, information, and IT systems. Section 1 states that "the policy establishes the enterprise risk management program that is commensurate with the importance and sensitivity of information resources to CDC's public health mission."

CDC has defined their mission with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. It can be found at: http://www.cdc.gov.

NIST Requirement b.

The Office of Safety, Security, and Asset Management (OSSAM) provides and maintains a secure work environment for CDC's global personnel through implementing and upholding best practices in physical and personnel security, emergency management, and intelligence operations activities.

OCISO has developed the CDC IT Security Program Implementation Standards which define the security controls that are integrated into the enterprise architecture through a robust, mature Security Authorization process.

Information protection needs are determined by examining of the mission/business processes against the security controls identified in the CDC IT Security Program Implementation Standards. The result is a set of security controls that must be applied to the associated information systems supporting the mission/business processes. This determination is made by a team consisting of the system owners, system stewards, and the Certifying Agent. The examining of the mission/business processes against the security controls identified in the CDC IT Security Program Implementation Standards is performed until the security controls in place provide an acceptable level of risk to the protection of the mission/business processes.

2.5.12 PM-12 Insider Threat Program

Control Implementation Status: In Place

Control Effectiveness: Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The Incident Response (IR) team is responsible for proactively addressing information system threats and vulnerabilities, as well as responding the information security incidents, regardless of their source.

Threat Monitoring – The ISO Team regularly monitors the environment via weekly and on-demand security scans of information systems components, using the Tenable Nessus suite of applications. In addition, the team maintains a number of monitoring tools that generate email alerts to the team, as described in control SI-4, “Information System Monitoring.”

Incident Handling - The IR Team is primarily comprised of Infrastructure and Security Operations (ISO) and Technology Support Services (TSS) personnel, but depending on each Incident, Project Officials and Human Resources Management may be involved to assist in the investigation, resolution, remediation and reporting of information security incidents.

The NORC IT Security Compliance Team has responsibility for creating and modifying the Incident Handling process and ensuring it is appropriately integrated into the NORC Incident Response Plan and the NORC Contingency Plan. The Team also Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

All NORC employees are trained in incident response in their role as an information systems user. IR training in this respect is delivered as part of the NORC’s IT Security Awareness training, which all staff must complete initially when they start employment at NORC, as well within every 365 days via refresher training, thereafter. Select NORC IT Staff are trained in incident response, relative to their daily, information system roles and responsibilities.

The CDC Enterprise:

OSSAM:

OSSAM implements an insider threat program that consists of an annual refresher course. The Public Health Intelligence Office (PHIO), located in the Office of Safety, Security and Asset Management (OSSAM), has developed web-based training to meet the requirements of EO 13587. The mission of this mandatory course is to equip badged CDC staff & contractors with the skills to recognize indicators associated with intelligence collection efforts and report suspicious behavior. This includes a cross-discipline insider threat incident handling team that team is able to collaborate with the Cyber Security Operations Center (CSOC).

OCISO:

There are security controls in place to detect and prevent overall malicious activity. The Cyber Security Operations Center (CSOC) staff proactively identifies and responds to incidents. The following technology has been deployed to protect CDC’s network:

- NetWitness
- Snort
- FireEye
- Symantec and Checkpoint Anti-Virus.

2.5.13 PM-13 Information Security Workforce

Control Implementation Status: In Place

Control Effectiveness: Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Administrator and users with escalated privileges are required to complete a minimum of 8 hours of additional security training per year. The required number of training hours per year increases with responsibility.

- TSS Help Desk – 8 hours
- ISO Server Administrators – 15 hours
- ISO Network Engineers – 15 hours
- TSS & ISO Directors – 25 hours
- Security Team – 25 hours

Training records are recorded and stored, by year on NORC's IT Administration shared drive.
NORC sponsors requisite offsite training for those personnel to accumulate skills and certification, where appropriate that enable information security goals.

The CDC Enterprise:

The Office of the Chief Information Security Officer (OCISO) Management & Program Analyst is responsible information security workforce development and improvement via the OCISO Qual Card program. Supervisors meet with employees and ensure understanding of the OCISO Qual Card program, which identifies position-based competencies and is designed to assess and identify training requirements and opportunities.

OCISO arranges information security and privacy training for selected information security professionals, such as ISSOs and security stewards. OCISO continuously identifies, plans, and schedules information security and privacy training through the Human Capital Resources and Management Office via the HHS Learning and Management System (LMS).

The Office of the Chief Information Security Officer (OCISO) Policy and Planning (P&P) IT Specialist is responsible for managing the OCISO role-based training (RBT) program for individuals assigned significant information security roles and responsibilities (SSR). The OCISO Standard for Significant Security Responsibilities and Role-Based Training describes SSR and RBT requirements. A link to this document can be found in the in the CDC IT Security Program Implementation Standards.

The Human Capital Resources and Management Office (HCRMO) provides standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions via the Individual Development Plan (IDP).

The Individual Development Plan (IDP) is a written version of each employee's plans for their future as a federal employee. An IDP facilitates a partnership between the employee and supervisor by encouraging two-way communication. It can serve as a roadmap for employees to reach their goals and it provides a record (which employees maintain and track) of education, training and developmental activities. At the same time, it helps CDC to anticipate its own future talent pool to meet its goals.

2.5.14 PM-14 Testing, Training, and Monitoring

Control Implementation Status: In Place

Control Effectiveness: Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC IT Security Compliance Manager is responsible for the development and maintenance of an annual information security program/project management plan that includes testing, training and monitoring tasks. The program management plan is used to communicate required activities to the ISO Engineering and Technical Support Services (TSS) teams in support of ongoing information security maintenance and compliance efforts. In addition, the schedule is a tool for ongoing maintenance of activity completion and reporting to the CIO and ISO Director (CISO).

The CIO, ISO Director and Information Owners may provide input into specific program activities, based on client requirements and risk assessments to emphasize and prioritize certain activities, and realign the schedule, when resource constraints limit the ability to accomplish all scheduled activities. The IT Security Compliance Supervisor must update the schedule and any associated plan documents accordingly. Conversely, tasks may be added for increased training, testing and monitoring activities for systems deemed to be “higher risk.”

The CDC Enterprise:

NIST Requirement a.

The OCISO Cyber Security Action Plan (CSP) provides a process for ensuring OCISO develops, maintains and executes security testing, training, and monitoring activities associated with organizational information systems. Programs or actions that are integrated through the CSP include:

Testing
- Internal IT Security Audit Program
- Commissioning and coordinating independent penetration tests Training
- Security Awareness Training program
- Role-Based Training program
- Privacy Awareness Training program

Monitoring
- Enhanced Security Control Assessment (ESCA)
- Reviews of CDC’s IT Security Weakness POA&Ms
- Incident Response and Monitoring
- Continuous Monitoring Program

Additional mechanisms that support CDC developing, maintaining and executing activities associated with organizational information systems include:
- Contingency Plan testing as part of the Security Assessment and Authorization (SA&A) process [monitoring, testing]
- Information system-related actions under the Continuity of Operations Planning at CDC policy [testing, training]
- Scans and assessments conducted in accordance with the:
- OCISO Level III Workstation Software Security Evaluation Standard Operating Procedure.
- OCISO Vulnerability Remediation Framework Standard

NOTE: A link to these documents can be found in the CDC IT Security Program Implementation Standards. [monitoring, testing]
- Implementation of tools, training and processes supporting static code analysis [monitoring, testing]
- SAT. The Information Security Awareness Training is made available on the CDC intranet to educate CDC personnel to the common schemes (e.g., electronic, psychological, or physical) employed by unscrupulous computer types, which can cause harm to CDC systems or lead to the compromise of personally identifiable information. New CDC employees and contractors are required to complete the full course. Current employees and contractors who have completed the course in previous years are required to take only the refresher course. Employees who fail to complete this course by the specified date for each year will have their access to CDC's internal network suspended. [training]
- OCISO continuously identifies, plans, and schedules information security and privacy training through HRO / HHS LMS [training]
- RBT. Recognizing that effective education can expedite and improve security compliance, the SA&A Team accomplishes security training mandates by delivering information with attentive consideration of CDC computer user diversity. The SA&A Team increases security knowledge of CDC leaders and IT professionals that encourages them to embrace a culture that understands, accepts, and supports security initiatives. Therefore, accomplishment of role-based training objectives and the encouragement of educational credential development for CDC security professionals are prominent SA&A Team goals.

NIST Requirement b.

The OCISO Cyber Security Action Plan provides a process for ensuring OCISO security testing, training, and monitoring activities associated with organizational information systems are executed in a timely manner. It establishes tasks and milestones for when individuals or organizations are expected to complete designated activities.
Additional mechanisms that support timely execution of CDC security testing, training, and monitoring activities associated with organizational information systems include:
• The CISO's monthly between OCISO and ISSO's [monitoring, training]
• Stage Gate Reviews for IT projects that are implemented under the Enterprise Performance Lifecycle (EPLC) process [monitoring, training]
• Coordination and direction resulting from recurring meetings of the CDC Information Resources Governance Council and its subordinate committees [monitoring]
• The Information Security Awareness Training course is updated each year to address new mandates from the President's Office of Management and Budget, the Department of Health and Human Services, and other sources. [training]

2.5.15 PM-15 Contacts with Security Groups and Associations

Control Implementation Status: In Place

Control Effectiveness: Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The ISO Director (CISO) is a standing member of the Forrester Research Security and Risk Council, which provides NORC with a network of business and government peers, who convene to discuss security issues and best practices in security management.
The NORC Security Team includes trained and accredited personnel, who must participate in ongoing security training to maintain their credentials. NORC Security subject matter experts are responsible for generating the content and administering the NORC IT Security Awareness Training, which is delivered to the entire company in April of each year.

Further, NORC ISO Administrators and Engineers receive vendor training upon the implementation of security system components

NORC receives communication from all their major vendors on any security threats, vulnerabilities and patches.
NORC IT personnel receive alerts as they are issued from the following sources:
- SANS
- Microsoft Security Bulletin Advance Notification Service
- US-CERT mailing lists
- Technical Cyber Security Alerts
- Cyber Security Bulletins
- Cyber Security Alerts
- Cyber Security Tips

The CDC Enterprise:

NIST Requirement a & b.

The OCISO Cyber Security Operations Center (CSOC) Lead establishes and maintains contact with the following selected groups and associations within the security community:
- Government Forum of Incident Response and Security Teams (GFIRST)

- Unites States Computer Emergency Readiness Team (US-CERT)
- Federal Information Security Systems Educators Association (FISSEA)
- ActiveTrust Threat Intelligence Data (IID)
- iSIGHT Cyber Threat Intelligence Services

The OCISO CSOC Team Lead and staff attend conferences and obtain information associated with these entities which provides for ongoing security education and training.

NIST Requirement c.

The OCISO CSOC Team shares current security-related information including threats, vulnerabilities, and incidents with US-CERT, third-party vendors (IID), and Law Enforcement when applicable, while taking into consideration sensitivity of information shared.

2.5.16 PM-16 Threat Awareness Program

Control Implementation Status: In Place

Control Effectiveness: Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC performs real time alerting, daily anti-virus scan reports, firewall threat report and weekly vulnerabilities scan to identify any threat to any systems. The threats are shared with other IT groups and projects. NORC does not typically share any of this data with any 3rd parties, but does participate in investigations of breaches and incidents and will cooperate with requests for information, so long as it doesn’t compromise our security posture or the data within our custodial care.

The CDC Enterprise:

The OCISO Cyber Security Incident Response Team (CSIRT) conducts a monthly Unclassified Threat Awareness Briefing. The briefing includes cross-organizational presence of the Information Technology Services Office (ITSO) and other entities as pertinent to each briefing. Threat events and lessons learned are shared on a case-by-case basis, taking into consideration sensitivity of information shared.

3.0 OPERATIONAL CONTROLS

3.1 Security Awareness and Training (AT) Controls

3.1.1 AT-1 Security Awareness and Training Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled "Awareness and Training Policy" which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Awareness and Training.
The NORC Security Policy Awareness and Training Procedures contains documented procedures to facilitate the implementation of the Awareness and Training policy and associated Awareness and Training controls.
.
Continuous Monitoring – NORC reviews NORC-wide policies and procedures annually, which NORC defines as within every 365 days. If any changes are made, NORC policy and procedures are adjusted accordingly.

3.1.2 AT-2 Security Awareness, including Enhancement AT-2(2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC delivers Security Awareness Training to all users:

a. Within the first 30 days of hire;
b. In the event that a system change would prompt a change to the state of the organization's information security profile and require stronger diligence on the part of its employees, partners and subcontractors; and
c. Annually in the month of April.

Every new hire receives information Security Awareness Training and Privacy (Data Use Agreement) Training within the first 30 days of their employment at NORC.

NORC ISO Group and Privacy Office administers organization-wide Information Security Awareness Training and Privacy Training to all employees at least every 365 days, and as needed when significant system changes or practices occur that necessitate security or privacy protocol changes.

NORC's Security Awareness Training includes content about potential threats attributed to insider attack; those incidents that may occur as a result of inadvertent, unplanned carelessness or from malicious activity. The training points out system and human characteristics and behaviors that could indicate a pending threat. The training directs users to report potential violations without fear of reprisal through a variety of possible internal channels to trigger prompt handling of probable or realized incidents.

3.1.3 AT-3 Role-Based Security Training

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Every new hire receives information security training within the first 30 days of their employment at NORC. NORC provides Organizational role-based, security training for management, operational, and technical roles and related responsibilities covering physical, personnel, and technical safeguards and countermeasures. System Administrators and Project Team members must complete agency-specific security training as mandated by some federal agencies prior to accessing systems or data.

NORC IT Security role-based training is conducted on a quarterly basis and IT Personnel must complete their quarterly training by the end of every quarter during the calendar year.

Initial Role-based IT Security training is conducted within one month after IT personnel start work at NORC in order to complete the training prior to gaining privileged access to NORC IT systems and/or software. Additionally, when system and software changes have IT Security impact, personnel with responsibilities for that system or software must undergo training relative to those changes. Information Security training for all employees is conducted at least every 365 days.

3.1.4 AT-4 Security Training Records

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC documents and monitors organization-wide IT Security Awareness Training and Privacy Training, as well as targeted, role-based specific information security training.

By default, NORC maintains IT security training records for a minimum of three years. Regarding Agency-mandated IT security training, NORC project managers also retain individual training records of completed training by employees for durations stipulated by the Agency, contract or project for which the training was competed.

3.2 Configuration Management (CM) Controls

3.2.1 CM-1 Configuration Management Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Configuration Management Policy” which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Configuration Management

The NORC Configuration Management Procedures contains documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

NORC update its Configuration Management policies and procedures annually, defined by NORC as within every 365 days.

3.2.2 CM-2 Baseline Configuration, including Enhancements CM-2(1) (3) (7)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC establishes baseline configurations for its information systems related components including the consideration of communications and connectivity- related aspects of its systems. The baseline configuration of the information system is consistent with the organization’s enterprise architecture.

NORC reviews and/or updates the baseline configurations of its information systems at least annually, when there is a major change or update, upgrade to the system, or when there any baseline configuration checklists or hardening guidelines adopted are updated. NORC baseline configurations are also reviewed and/or updated as an integral part of the information systems component installations.

Older versions of baseline configurations are saved in all encrypted backups and can be rolled back if necessary.

NORC Technology Support Services configures laptops with security targets that conform to NIST 800-53 Rev. 4, FIPS 140-2 and the United States Government Configuration Baseline (USGCB) standards, with some documented exceptions in the NORC laptop baseline. When laptop configurations are built, an ISO System Engineer scans a test laptop using Nessus Security Center to identify any vulnerabilities that may exist. Configurations may be modified until a successful scan is attained. Only after an acceptable Nessus scan is certified by the System Engineer will the baseline be established and deployed to production laptops. This hardening protocol ensures that regardless of the risk associated with certain geographic areas, laptops are sufficiently secured to protect the confidentiality of data stored on the devices, and risks associated with malicious code are minimized.

When project laptops are returned to NORC, TSS runs “dump scripts,” which zip the project data content of the laptops to secured network folders, tied to an assigned device ID. This procedure facilitates the retention of the project data, and allows TSS to reconfigure and redeploy the laptops for future projects.

3.2.3 CM-3 Configuration Change Control, including Enhancement CM-3(2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

The NORC IT Engineering Division maintains an IT system configuration change capability that includes the review of system and software baseline changes. Changes take place on a daily basis and are communicated amongst Engineering Team members. The status of changes and any obstacles to implementing configuration changes are addressed during weekly CM meetings, and amongst Engineering Team Leads, the IT Security Compliance Team and the IT Engineering Director for more pertinent issues that cannot wait until weekly meetings.

The medium by which NORC conducts change control is the BMC Footprints Service Management application. NORC uses the Configuration Management Tracking queue in BMC Footprints to document, review and approve configuration-controlled changes to the system. Documentation records of configuration-controlled changes to the system are retained for no less than a year and records of configuration-controlled changes to the system are reviewed for quality and completion. Changes are peer reviewed and sent to the change control committee before it is implemented. Only approved changes are implemented.

NORC retains records of configuration-controlled changes to the information system for no less than a year.

The logging and retention of records of configuration changes allows the NORC IT Engineering Department to audit those changes to the systems at any time.

NORC coordinates and provides oversight for configuration change control activities through the Configuration Change Control Committee that convenes weekly every Wednesday morning, in advance of scheduled Wednesday evening IT maintenance windows.

The NORC IT-94 Security Configuration Settings Standard Operating Procedure (SOP) provides the documented process for implementing changes to the operating system with the Security Impact Analysis as appropriate.

3.2.4 CM-4 Security Impact Analysis

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
As part of its Change Management process, NORC IT conducts a Security Impact Analysis (SIA) prior to authorization of any changes in order to determine the potential security impact to the Information System. The NORC IT Change Control Group uses the SIA as a key factor in change authorization or rejection decisions. An audit process form is completed and reviewed after the change is implemented.

3.2.5 CM-5 Access Restrictions for Change

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Only administrators can implement changes to code. NORC utilizes their helpdesk ticket system to track system changes in an automated manner. The system tracks the change owner, test results, the purpose of the change, and servers or systems affected by the change, and any ancillary documentation for that change. Changes are peer reviewed and sent to the change control committee before it is implemented.

3.2.6 CM-6 Configuration Settings

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC IT-94 Security Configuration Settings (CM-6) Standard Operating Procedure (SOP) provides the documented process for implementing configuration changes to the operating system. The accepted or mandatory security configuration settings for NORC IT products employed within NORC information systems reflect the most restrictive mode per operational requirements, and reflecting CIS published hardening standards.

NORC implements Microsoft Best Practices, CIS Benchmarks, USGCB, Nessus and VMCenter Protect Shavlik Patch Manager for security configuration settings.

The accepted or mandatory security configuration settings for NORC IT products employed within NORC information systems reflect the most restrictive mode per NORC Configuration Management Plan requirements. NORC must identify, document and approve any exceptions to the mandatory security configuration settings for individual components within its information systems based on explicit operational requirements.

eIQ SecureView is NORC’s Security Incident and Event Management (SIEM) tool, which detects unauthorized and security-relevant information, and which may trigger the NORC Incident Response capability where NORC IT incidents are concerned, ensuring detected events are tracked, monitored, corrected, and available for historical purposes. The NORC IR Plan outlines the detection of unauthorized, security-relevant configuration changes into the organization’s incident response capability to ensure all such detected events are tracked, monitored, corrected, and available for historical purposes.

3.2.7 CM-7 Least Functionality, including Enhancements CM-7(1) (2) (4)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC monitors configuration settings regularly in line with the data collection schedule, provides reporting to project managers to monitor access levels, has an annual review and on request reporting of all permissions throughout the HHS system components. NORC considers least privilege and least functionality when reviewing baseline configurations as an integral part of the information systems component installation process.

All NORC systems are protected from unauthorized access by a layered system of boundary routers and hardware firewalls. Ports are only opened in the boundary layer, by request, if there is an explicit business need. All unencrypted authentication network protocols are prohibited. NORC reviews and/or updates the baseline configurations of its information systems, when there is a major change or update, upgrade to the system, or when any adopted baseline configuration checklists or hardening guidelines are updated.

As a part of the Center for Internet Security (CIS) Annual Baseline Review, NORC checks for unnecessary ports, protocols, functions, and services within the NORC baselines and security checklists. If identified, unnecessary ports, protocols, functions, and services are not incorporated the CIS baseline.

The information system prevents execution in accordance with project requirements that determine the rules authorizing the terms and conditions of software program usage. NORC limits access to systems in accordance with least privilege principles.

3.2.8 CM-8 Information System Component Inventory, including Enhancements CM-8(1) (3) (5)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC maintains a system inventory as part of the Configuration Management (CM) Plan. All parts of the information system are maintained as part of asset management in an on-line database server inventory. The inventory includes defined information deemed necessary to achieve effective information system component accountability, i.e., • Unique Identifier and/or Serial Number • Information System (IS) of which the component is a part • Type of IS component (e.g., server, desktop, application) • Manufacturer/ Model information • Operating System Type and Version/Service Pack Level • Presence of virtual machines • Application Software Version/License information • Physical location (e.g., building/room number) • Logical location (e.g., IP address) • Owner • Operational status • Primary and secondary administrators • Primary user.

Inventories are reviewed periodically and project inventories are maintained in the configuration management plan, which is available upon request.

NORC updates the inventory of information system components as an integral part of component installations, removals, and information system updates. When a part of a NORC information system is changed, this change must be reflected in the system boundary information system component inventory and on-line asset management database.

NORC utilizes inventory management and network scanning tools to detect the presence of unauthorized hardware, software and firmware components within the information system. The inventory management tool alerts the ISO Server Administration Team, who takes appropriate actions to remove the unauthorized system from the environment.

In the event that an unauthorized information system is found within the NORC environment, IT Management may invoke the Incident Response process to determine what happened and resolve the issue.

NORC verifies that all components within project authorization boundaries of the information system are inventoried as a part of the system. NORC updates the inventory of information system components as an integral part of component installations, removals, and information system updates. When a part of a NORC information system is changed, this change must be reflected in the system boundary, information system component inventory and on-line asset management database.

3.2.9 CM-9 Configuration Management Plan

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC Configuration Management Plan addresses roles, responsibilities, and configuration management processes and procedures.

NORC defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management.

NORC establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

The CM plan has a section for the Change Management process which shows how changes through the change management process are done, how configuration settings and configuration baselines are updated. The Configuration Management plan is maintained in a secure network location with limited access.

3.2.10 CM-10 Software Usage Restrictions

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
From the NORC General Information Technology Policy, “Installation of software on NORC computers is closely controlled. NORC prohibits the installation or downloading of any software program unless reviewed and approved by the Technical Support Services (TSS) Department prior to installation. Employees who are aware of a program or application that may be useful should notify the TSS Department so that the software may be evaluated. Unauthorized software or software for non-business purposes should not be placed on NORC hardware.”

TSS locks down computers to prevent users from installing any software on their devices, without involvement of users with administrative credentials and rights.

NORC IT Staff manages the inventory of software licenses in accordance with the asset tracking procedures defined in control CM-08 (1). License keys and counts for desktop software are stored within BMC Footprints – Software Licensing module, except for server-level Microsoft license inventories, which are managed directly in Microsoft's Volume Licensing Service Center (VLSC) internet site.

Purchase orders are typically attached to the license inventories in Footprints. All purchase receipts and purchase orders are retained by the NORC Accounting group.

NORC non-privileged users are unable to install peer-to-peer software without the assistance of a user with system administrator credentials. NORC users are not permitted to use these types of programs. Users are educated on the dangers and risks associated with these types of programs in annual Security Awareness Training.

3.2.11 CM-11 User-Installed Software

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC General Information Technology Policy states, "Installation of software on NORC computers is closely controlled. NORC prohibits the installation or downloading of any software program unless reviewed and approved by the Technical Support Services (TSS) Department prior to installation. Employees who are aware of a program or application that may be useful should notify the TSS Department so that the software may be evaluated. Unauthorized software or software for non-business purposes should not be placed on NORC hardware."

The NORC Information Systems Usage Policy states, "Installing unauthorized software applications, tools, utilities, File Transfer Protocols (FTP) and other Internet access protocols, Internet programs, remote control, terminal access, or bulletin board type programs on a NORC computer is prohibited…. Violations of this policy may result in disciplinary action including loss of applicable privileges, termination of employment, and referral for criminal prosecution or civil action. Individuals who violate standards may also be required to reimburse NORC for losses or damages resulting from the violation."
These policies are provided to new NORC employees as part of onboarding. They are made available at all times on the NORC Insite Intranet policy portal. The concepts are reiterated every 365 days through IT Security Awareness Training.

TSS locks down computers to prevent users from installing any software on their devices, without involvement of users with administrative credentials and rights.   NORC enforces software installation policies through security controls such as Active Directory group policies and Access Control Lists.

NORC TSS Help Desk reviews the software installed on endpoint devices against its whitelist of approved software monthly.

3.3 Contingency Planning (CP) Controls

3.3.1 CP-1 Contingency Planning Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Contingency Planning Policy” which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Contingency Planning.
The NORC Security Contingency Planning Procedures contains documented procedures to facilitate the implementation of the Contingency Planning policy and associated Contingency Planning controls.

Continuous Monitoring – The Contingency Planning Policy and Procedures are reviewed and updated as necessary at least every 365 days.

3.3.2 CP-2 Contingency Plan, including Enhancements CP-2(1) (3) (8)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
N/A – This system has “low” availability and chooses not to recover during BCP events. A Non-Recovery BCP form has been submitted in support of this system’s authorization. This form is reviewed, updated, and resigned annually.

3.3.3 CP-3 Contingency Training

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
N/A – This system has “low” availability and chooses not to recover during BCP events. A Non-Recovery BCP form has been submitted in support of this system’s authorization. This form is reviewed, updated, and resigned annually.

3.3.4 CP-4 Contingency Plan Testing and Exercises, including Enhancement CP-4(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:

N/A – This system has “low” availability and chooses not to recover during BCP events. A Non-Recovery BCP form has been submitted in support of this system’s authorization. This form is reviewed, updated, and resigned annually.

3.3.5 CP-6 Alternate Storage Site, including Enhancements CP-6(1) (3)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC establishes an alternate storage site including necessary agreements to permit the storage and recovery of backed-up information system data. The present NORC alternate storage site is at Iron Mountain, 1565 Hunter Road, Hanover Park, IL 60133, which is approximately 23 miles away from NORC primary processing site at 1808 Swift Drive, in Oak Brook, IL. NORC maintains an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards as the primary site in the event of a contingency. NORC identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions which are delineated in the NORC Contingency Plan and the Disaster Recovery Plan.

Data stored offsite is on digital media and is encrypted at-rest at the alternate storage site as well. Iron Mountain provides a secure environment for the storage of the encrypted tapes.

3.3.6 CP-7 Alternate Processing Site, including Enhancements CP-7(1) (2) (3)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC maintains an alternate processing site in a separate and distinct Zayo data center, on Oak Brook, IL. While physically located in the same building as NORC’s primary information systems, the alternate processing site is protected by separate power systems (UPS and generator) and other environmental controls, as described in controls PE-09 – PE-15. NORC’s recovery time objective (RTO) for converting mission critical functions and services to the alternate processing site is 24 hours and 72 hours for other essential services. The recovery point objective (RPO) is 24 hours. This is based requirements set forth by business partners and defined in the Business Impact Analysis.

NORC’s alternate processing site is a warm site. NORC System Engineers are allowed 24x7 access to the site. Zayo provides a robust data center environment, with multiple levels of environmental controls redundancy to minimize the likelihood of a full failure. Zayo is contractually responsible for ensuring availability of data center infrastructure services on a 24x7 basis. NORC System Engineers are solely responsible for the cut over of services to the alternate processing environment.

In April 2015, NORC security personnel conducted an onsite assessment of Zayo's data center physical and environmental controls, and attest that the equipment and supplies in the alternate processing site will support NORC's business in a contingency scenario.

While physically located in the same building as NORC's primary information systems, the alternate processing site is protected by separate but equivalent power systems (UPS and generator) and other environmental controls, as described in controls PE-09 – PE-15. NORC plans to migrate the alternate processing capabilities to an alternate Zayo data center, in Ashburn, Virginia.

NORC identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions which are also detailed within the contingency plan and related documents.
Hazards that might affect the alternate systems are defined in the organizational risk assessment, the contingency plan, the Disaster Recovery Plan (DRP), and Business Impact Analysis (BIA).

3.3.7 CP-8 Telecommunications Services, including Enhancements CP-8(1)(2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has established a contractual relationship with AT&T to provide telecommunications circuits into NORC facilities, including the Zayo data center. The two primary DS3 circuits arriving at the Zayo data center traverse separate and distinct fiber paths, terminating at distinct fiber vaults located in different locations within the Zayo facility.

NORC Network Engineers continue to develop technical capabilities with Session Initiation Protocol (SIP) to take advantage of the redundancy that Voice over Internet Protocol (VoIP) provides. The data circuits that support this traffic are provided by Global Crossing.

Data circuits are segmented within the Zayo data center to provide network connectivity to both the primary and alternate data processing facilities.

Cross-connect change requests require a ticket to the Zayo Network Operations Center, which is staffed locally. Cross-connection facilities are locked in a secure room, and only Zayo personnel have access to that space. NORC's goal is to restore all mission critical services within 24 hours of a contingency event.

3.3.8 CP-9 Information System Backup, including Enhancement CP-9(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC backs up user-level information contained in the information on a daily basis, consistent with

RTOs and RPOs.   NORC's backup schedule consists of incremental daily backups and a weekly full backup. Backups are stored on dedicated disk array located in the primary data center (daily), alternative processing site disk array (daily) and to encrypted tape media for offsite storage (monthly). Full procedural documentation is available in NORC SOP, IT-154, "Information Back-up." Information System Backup

NORC backs up system-level information, including documentation and archived versions of information systems on a daily basis, consistent with RTOs and RPOs. NORC's backup schedule consists of incremental daily backups and a weekly full backup. Backups are stored on dedicated production disk array (daily), alternative processing site disk array (daily) and to encrypted tape media for offsite storage (monthly).

NORC backs up information system documentation, including information security documentation on a daily basis, consistent with RTOs and RPOs. NORC's backup schedule consists of incremental daily backups and a weekly full backup. Backups are stored on dedicated production disk array (daily), alternative processing site disk array (daily) and ton encrypted tape media for offsite storage (monthly).

NORC maintains three distinct backup locations. The primary site is on a dedicated disk array in NORC's production environment, within the Zayo data center. The secondary site is on NORC's dedicated array in the alternate processing facility, in a separate data center of the Zayo facility. Finally, NORC utilizes CommVault's encrypted backup functionality to save backups to tape. Those media are stored offsite at a secure Iron Mountain storage facility. NORC's backup locations provide physical security of the backups as described in the NORC's Physical and Environmental Protection Policies and Procedures. All backups are restricted to designated NORC ISO Engineering personnel. In addition to physical security, NORC employs the concept of least privilege as defined in NORC Least Privilege (AC-6) SOP for access to information system backups.

NORC executes system and data restores from backup on at least an annual basis, as part of contingency plan exercises, with full documentation of results. When testing reliability and information integrity, NORC personnel follow contingency planning procedures in order to ensure an accurate test of NORC information system backups. Additional tests may be executed based on the following conditions:

- Significant change to the information system and/or backup system
- Migration of data center components
- Request of client agency or 3rd party auditor
- Re-test following a prior failed test
- Change in the Contingency Plan protocols

NORC must test backup information annually to verify media reliability and information integrity. When testing reliability and information integrity, NORC personnel follow contingency planning procedures in order to ensure an accurate test of NORC information system backups.

3.3.9 CP-10 Information System Recovery and Reconstitution, including Enhancement CP-10(2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Recovery and reconstitution capabilities employed by NORC are a combination of automated mechanisms and manual procedures. For workstations, laptops and mobile devices, NORC uses automatic deployment of system images and standard software. Windows server deployments use system images and software installed manually. All systems are configured to automatically adhere to the baselines described in NORC IT-18 Baseline Configuration (CM-2) SOP.

The transaction based systems in the NORC information are NORC's databases. NORC databases support and implement transaction recovery using CommVault vendor provided tools.

3.4 Incident Response (IR) Controls

3.4.1 IR-1 Incident Response Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Incident Response Policy” which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Incident Response. The policy is distributed to: NORC IT Management, ISO and TSS personnel, the Institutional Review and Data Governance Boards and the Chief Privacy Officer.

The NORC Security Incident Response Procedures contains documented procedures to facilitate the implementation of the Incident Response policy and associated Incident Response controls.

NORC reviews its Incident Response Policies and Procedures annually, which is defined by NORC as within every 365 days.

3.4.2 IR-2 Incident Response Training

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
All NORC employees are trained in incident response in their role as an information systems user. IR training in this respect is delivered as part of the NORC’s IT Security Awareness training, which all staff complete initially when they start employment at NORC, as well as annually via refresher training, thereafter. NORC defines ‘annually’ as within every 365 days.

The IT Security Awareness training includes content that teaches employees how to identify threats, suspicious activities or other occurrences from external or internal sources which may constitute an incident. Employees are also instructed on how to respond to such incidents. NORC does have a centralized incident response reporting function. Users are directed to call the Telephone Surveys & Support Operations (TSS) or email IRC@norc.org.

Select NORC IT Staff are trained in incident response, relative to their daily, information system roles and responsibilities. IT Staff must not only know how to identify a suspected incident, but also how to verify that an incident has indeed occurred, and how to respond accordingly once an incident has been positively identified.
IT Staff undergo annual training that is related to the incident response process mentioned below. Such IR training can also take place as part of the annual contingency plan exercises.

In the event of a suspected incident, users are generally directed to call TSS or email IRC@norc.org. All incident reports are documented by the IT Security Compliance team. Users can also open up a

TSS help desk ticket but must ensure the subject line of the ticket contains verbiage identifying it a security incident or suspected security incident.

Once the incident has been confirmed, the IT Security Compliance team assigns the incident to the appropriate IT staff member or members, with an incident criticality and proposed timeframe for resolution. The designated IT staff responds to IT Security Compliance team within the proposed timeframe with a resolution proposal and provide updates to the IT Security Compliance team until the incident is fully remediated.

3.4.3 IR-3 Incident Response Testing, including Enhancement IR-3(2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC tests incident response at least every 365 days through exercises with current incidents and simulated attacks using software during security audits. Table-top exercises are simulated throughout the year in recovery scenarios with various system types: database and server recovery, virus attacks, equipment failures, reported laptop loss.

NORC conducts any technical information security testing and assessments, such as penetration testing or assessments; NORC IT uses the opportunity to test its IR capability, depending on the type of simulated attack.

3.4.4 IR-4 Incident Handling, including Enhancement IR-4(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC incident response team employs defined and documented Incident Response and Emergency Response Procedures for this capability including preparation, detection analysis, containment, eradication, and recovery.

The NORC IT Security Compliance Team has responsibility for creating and modifying the Incident Handling process and ensuring it is appropriately integrated into the NORC Incident Response Plan and the NORC Contingency Plan.

The Team incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Automated tools are in place to monitor firewalls and perimeter protection, as well as routers. What's Up Gold monitors all server activity, and Idera monitoring tool is deployed for all production databases. eIQ SecureVue (SIEM) monitors the overall security posture of the network and provides alerts to the ISO Engineering team. Incident response team members are automatically notified when incidents occur.

3.4.5 IR-5 Incident Monitoring

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.
Documenting information system security incidents can include, incident details, status of the incident, other pertinent information necessary for forensics, evaluation of incident details, trends, and handling, as well as maintaining records about each incident. An incident response form is maintained which documents the details of each significant incident.

3.4.6 IR-6 Incident Reporting, including Enhancement IR-6(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC requires employees to report suspected security incidents to the NORC Incident Response Team as soon as it's known. NORC IR must, in-turn, confirm the validity of the potential incident and, if legitimate, report the details of the incident to designated authorities immediately, especially if the information involves NORC systems that process and store sensitive Federal Agency data, such as PII or PHI data. Designated authorities generally include the Federal Agency representative or even Law enforcement, in some cases.

NORC Management is responsible for reporting confirmed security incidents to Federal Agency program managers immediately upon discovery or according to specified project specific guidelines.

Automated tools are in place to monitor firewalls and perimeter protection, as well as routers. What's Up Gold monitors all server activity, and Idera monitoring tool is deployed for all production databases. NORC employs automated tools SecureVue eIQ Security Incident and Event Management System (SIEM), Varonis and McAfee ePolicy Orchestrator (ePO) to assist with incident identification. Incident response team members are automatically notified and paged when incidents occur.

3.4.7 IR-7 Incident Response Assistance, including Enhancement IR-7(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC's Intranet contains a link to advise users on how to report incidents to the appropriate personnel. This link also provides an email, ir.norc.org, for reporting incidents.

NORC's annual IT Security Awareness Training contains information related to incident response including how to identify an incident and to whom it shall be reported.

3.4.8 IR-8 Incident Response Plan

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
IT Security Compliance team provides the organization with a roadmap for implementing its incident response capability. The Incident Response Plan describes the structure and organization of the incident response capability, and: Provides a high-level approach for how the incident response capability fits into the overall organization; Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; Defines reportable incidents; Provides metrics for measuring the incident response capability within the organization. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and is reviewed and approved by the NORC VP of IT and the ISO and TSS Directors. The NORC Incident Response Plan includes protocols for the handling of privacy-related incidents.

Copies of the Incident Response Plan are distributed to NORC IT Management and the Chief Privacy Officer on at least an annual basis. The NORC ISO Engineering Team provides the Incident Response Plan to federal agency clients upon request. The IT Security Compliance Supervisor prepares a redacted draft for distribution to the Data Governance Board and the Institutional Review Board Manager on an annual basis.

The ISO Incident Response Team reviews and revises the Incident Response Plan at least every 365 days to address system/organizational changes or problems encountered during Plan implementation, execution, or testing.

The NORC Incident Response Plan is a living document that reflects the current NORC information systems environment. The plan includes the latest protocols, which have been revised over time to address any procedural issues that have been identified in prior versions, which may have been difficult to manage.

NORC Communicates Incident Response Plan changes to all persons with plan responsibilities. Team leaders are responsible for ensuring all employees in their unit are aware of policies and procedures for protecting personal and confidential information.

The Plan is protected from unauthorized disclosure and modification via file access rights.

3.5 Maintenance (MA) Controls

3.5.1 MA-1 System Maintenance Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Maintenance Policy” which defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities/personnel (i.e., the system administrators, ISSOs, system owners/business owner, and users), and compliance.

The NORC Security System Maintenance Procedures contains documented procedures to facilitate the implementation of the System Maintenance policy and associated System Maintenance controls.

Continuous Monitoring – NORC reviews organization-wide policies and procedures annually, which NORC defines as within 365 days. If any changes are made, NORC policy and procedures are adjusted accordingly.

3.5.2 MA-2 Controlled Maintenance

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC uses the BMC Footprints Helpdesk software for tracking controlled maintenance and repair activities of NORC IT components. Footprints Helpdesk is used to create maintenance records and schedule maintenance actions, document progress for those actions, as well as review maintenance activities that have been performed. The policy and associated procedures are provided to NORC ISO and TSS teams with responsibilities for systems maintenance.

Most all maintenance and repair actions are controlled and completed within NORC’s Network Operations and Technology Center (NOTC) located in Chicago, NORC’s data center within Zayo facilities at 1808 Swift Drive, Oak Brook, IL, and infrequently at other NORC locations. In some cases, maintenance is performed remotely by vendors where the vendor is either granted remote access to components and performs the maintenance or repairs, or monitored by NORC IT Staff while remotely logged in to NORC IT Staffs systems.

On the intermittent occasions when NORC IT systems or components of those systems require maintenance, repair or disposition apart from the NORC primary data center or other NORC location where they have been employed, NORC ISO is responsible for explicitly approving removal of such IT components from NORC facilities. For release of IT equipment outside of NORC facilities, a NORC property pass must be completed by the NORC ISO prior to release of the equipment which properly identifies the asset(s) being removed.

Should NORC IT equipment require maintenance or repair outside NORC organizational control, such equipment will be sanitized to remove all information from the associated media prior to being released outside of NORC facilities. NORC currently uses BC-Wipe to sanitize such equipment media, which overwrites existing data three times.

Once maintenance and repair actions are finished and the IT equipment has been returned to NORC for use, ISO personnel must ensure the all security controls are employed on the equipment prior to the equipment’s redeployment to the Production environment. This includes following security checklists, configuring servers with CIS benchmark settings, applying patches, applying security configurations, and installing antivirus software and encryption software.

Maintenance activities are recorded using the Footprints software. Footprints maintenance records maintain granular information to accommodate specific maintenance queries including:

- Date and time of maintenance
- Name of the individual performing the maintenance
- Name of escort (if necessary)
- Description of the maintenance performed
- List of equipment removed or replaced (including identification numbers, if applicable)

3.5.3 MA-3 Maintenance Tools, including Enhancements MA-3(1) (2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC certifies, controls, and monitors the use of information system maintenance tools for certified equipment and maintains the list of certified tools on an ongoing basis. Maintenance tools are monitored weekly and any changes must go through change control process.

NORC ISO personnel must inspect all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. This inspection must be made prior to the tools entering the area (room, closet, lab, etc.) containing the information system.

NORC personnel scan all media or files containing diagnostic and test programs for malicious code, on an isolated system, before the media or files are used in the information system.

3.5.4 MA-4 Nonlocal Maintenance, including Enhancement MA-4(2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
ISO Directors, System owners or their delegates are responsible for approving system access and maintenance activities. Typical non-local maintenance activities include remote patch deployment and virus definition updates.

No non local maintenance tools are used without the approval of the ISO Director.

Users accessing the system from outside the NORC network must use the NORC provided VPN gateway, digital certificate, and Active Directory accounts.

NORC IT Security Compliance team regularly audits maintenance requests and access logs.

All system maintenance activities must begin and be terminated as documented in the change control ticket, which is authorized prior to implementation by the NORC IT Change Control Group.

NORC documents non-local maintenance and diagnostic connections standards and controls in its security plans, policies and procedures.

3.5.5 MA-5 Maintenance Personnel

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Maintenance personnel are required to be granted authorization from the Systems Team Leads or ISO Director before beginning work on any part of a NORC information system.

NORC ensures that personnel performing maintenance on an information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

In the case of an emergency maintenance situation where the maintenance personnel are not on the approved list, an existing approved member may grant temporary authorization for emergency maintenance subject to later review and approval by the Systems Team-Lead.

3.5.6 MA-6 Timely Maintenance

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The System obtains maintenance support and spare parts for all system components in production within 24 hours.
For standard NORC equipment, maintenance support and spare parts contracts exist and are assigned the following time frames depending on mission criticality:
High Priority = 0-4 business hours
Medium to Low Priority = Next business day

3.6 Media Protection (MP) Controls

3.6.1 MP-1 Media Protection Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Media Protection Policy” which defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational

entities/personnel (i.e., the system administrators, ISSOs, system owners/business owner, and users), and compliance.

The NORC Security Media Protection Procedures, contains documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Continuous Monitoring – NORC reviews NORC-wide policies and procedures annually, which NORC defines as within every 365 days. If any changes are made, NORC policy and procedures are adjusted accordingly.

3.6.2 MP-2 Media Access

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Access to sensitive areas including all NORC offices and server rooms are controlled and monitored. Only authorized personnel, with appropriate physical security credentials may access these facilities areas without escort.

3.6.3 MP-3 Media Marking

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC marks, in accordance with Organizational policies and procedures, removable information system media and information system output, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

As NORC is not a Government Agency, NORC limits media marking to only those information system components that remain in the data center(s). Removable media are exempt from media marking and/or labeling.

3.6.4 MP-4 Media Storage

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC physically controls and securely stores all sensitive information or data at rest within secure

facilities using both technical and physical security mechanisms.

NORC protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. NORC’s sanitization procedures are covered by NORC IT-104 Sanitization Procedures SOP.

3.6.5 MP-5 Media Transport, including Enhancement MP-5(4)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC ISO System Engineers protect and control all media with sensitive information, utilizing the CommVault backup and recovery system to write all manner of organizational data to LTO-4 magnetic tape data storage media. CommVault encrypts all backups with AES-256 data encryption, in accordance with FIPS 140-2 guidelines. Prior to transport, media are secured in locked containers, which remain locked until arrival at Iron Mountain (offsite storage vendor), where the boxed are opened, and each tape scanned as it is placed into inventory.

NORC contracts with Iron Mountain to provide off-site tape storage, which includes the transport from NORC facilities to Iron Mountain. Iron Mountain drivers take possession of encrypted backup tapes in securely locked transport cases for offsite storage and other media for on-site destruction under the supervision of NORC personnel. A full chain of custody control exists to track the location and possession of backup media while being transported from secure NORC facilities to the Iron Mountain storage facility, where it is inventoried and securely stored. Iron Mountain drivers scan boxes upon pickup and loading into the van. Iron Mountain vehicles are equipped with GPS, which allows Iron Mountain to monitor the location of their drivers and our tapes. When NORC Backup Administrators request media to be returned, Iron Mountain follows the same protocol in reverse.

All inventorying of tapes and accounting of activities associated with backup media are documented in the Iron Mountain Secure Sync system. All media set for destruction are sanitized, in accordance with the controls defined in MP-06. The NORC Backup Administrator logs an inventory of media for destruction, and receives certificates of destruction from NORC’s destruction vendors. Field Operations management tracks inventory of field laptops, including possession and location information. NORC Technical Support Services track inventory of corporate office laptops and encrypted removable media, including possession and location information.

Only named NORC IT Engineering and Iron Mountain personnel are authorized access to this media.

3.6.6 MP-6 Media Sanitization

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Media sanitization is addressed in the NORC Security Manual. All computer storage media that contains, or is believed to contain, data categorized as and/or sensitive is properly sanitized prior to disposal, transfer, and/or surplus. Computer storage media includes, but is not limited to: magnetic tape, floppy diskettes, optical media (CD and DVD), scanners, copiers, printers, notebook computers,

workstations, network components and mobile devices. Media not containing any sensitive data does not require sanitization prior to disposal. Sanitization methods vary, in accordance with specific requirements, but include: clearing (overwriting or wiping), purging (degaussing), or destroying (disintegration, pulverizing, shredding, incineration, etc.).

Media sanitization is performed using several different methods depending on the type of media being disposed, classification of the data it maintains, and whether the media will remain under organizational control.

3.6.7 MP-7 Media Use, including Enhancement MP-7(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC restricts the use of portable media on NORC information systems using WinMagic SecureDoc encryption tools. NORC classifies for different user types for portable media.

- Project Field Interviewers are provisioned with locked down laptops, whose external ports (USB, etc.) are completely disabled.
- Desktop Users can utilize encrypted USB flash drives (encrypted by WinMagic), but cannot use external hard drives.
- General Laptop Users can use both encrypted USB flash drives and external hard drives (encrypted by Win Magic).

Further definition can be found in NORC Policy K7 – Portable Media.

NORC has established strict controls over the use of portable media. When media with no identifiable owner is inserted into a NORC-owned device, WinMagic encrypts the drive before use, and the device becomes tied to the user’s primary NORC device. An encrypted device holding any data cannot be unencrypted without the WinMagic decryption key.

3.7 Physical and Environmental Protection (PE) Controls

3.7.1 PE-1 Physical and Environmental Protection Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Physical and Environmental Protection Policy” which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Physical and Environmental Protection.

The NORC Security, Physical and Environmental Procedures, contains documented procedures to facilitate the implementation of the Physical and Environmental policy and associated Physical and Environmental controls.

The PE Policy and its associated procedures are distributed to the NORC ISO, TSS, Facilities, Security and Senior Management teams.

The Physical and Environmental Protection Policy is reviewed at least every 365 days. The Physical and Environmental Protection Procedures are reviewed at least every 365 days.

3.7.2 PE-2 Physical Access Authorizations

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
An electronic list of access privileges is maintained. Changes to this directory must be documented and approved by the appropriate supervisor. NORC generates reports of access privileges on a regular basis which are reviewed by IT personnel.
Physical access to IT facilities is granted only to those with a recurring business need to access the specific area. ID card access is in place for specific locations housing critical telecommunications and IT equipment, and information systems.
After-hours access is secured by requiring sign-in to access the building.

NORC's primary data center is located in a secure cage inside the Zayo (formerly Latisys) data center, at 1818 Swift Drive, Oak Brook, IL 60523.

Zayo requires the NORC Single Point of Contact (SPOC) role to determine authorized users that will be granted access to the areas of Zayo that house NORC information systems. SPOCs complete access request forms through the Zayo tenant portal. Access privileges are maintained in Zayo's security / ERP system.

Entry to data center requires tenant and visitor sign in (including the surrender of a government issued ID card while on premise) at the Zayo NOC, use of RFID security badges and badge readers, biometric hand scanning, and mantraps. Additional identification validation for after-hours entry to Zayo's lobby (publicly accessible area).

NORC facilities - Through the use of Access It! (software) and the issuance of Kastle RFID cards, users are granted access to secure locations throughout the company. At Zayo, upon signing in, users surrender their government-issued ID card in exchange for an RFID security badge that facilitates access to only those areas in which NORC information systems reside. In addition, as part of the initial setup, authorized tenant users must register their hand scans into Zayo's biometric system. Actual data center access requires a biometric hand scan, a unique user PIN and the RFID badge.

Access It! privileged user access reports are reviewed on a monthly basis by the TSS and ISO Directors. The ISO Director reviews the NORC tenant authorized user list through the Zayo portal on a quarterly basis.

In the event of employee termination or transfer, security privileges can be adjusted or revoked immediately upon notification from management.

When a NORC employee who is an authorized user at Zayo leaves the company, or transfers to a department that is not responsible for physical information systems support, a NORC SPOC will remove access via the Zayo tenant portal.

3.7.3 PE-3 Physical Access Control

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:

NORC conforms to Zayo's defined controls to manage all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility.

At Zayo, a NORC Single Point of Contact (SPOC) pre-authorizes users within the Zayo tenant portal. Authorized Tenant personnel are provisioned with RFID badges that grant access only to the area(s) where NORC equipment resides. Upon arrival, authorized tenant personnel must check in with the Zayo NOC. The authorized user must surrender his/her government issued ID until the same access card is returned upon departure. Visitors must be authorized by a Latisys employee or a customer and are required to have an escort at all times.

After signing in, an authorized user must enter a pre-determined passcode and place his/her hand in a biometric scanner to gain entry to a mantrap. Once the first door closers, the user then swipes his/her RFID badge to exit through the other side, which allows access to the data center. After hours entry (6:00 pm – 6:00 am) requires a user to identify him/herself prior to building entry, stating name, organization and a pre-defined password via intercom communication to a NOC Engineer on duty. Tenant cages within the data center are locked and require an authorized badge swipe to gain entry or exit. Vendors must be pre-authorized by a designated NORC representative to either access a cabinet or to be escorted by an authorized facility employee.

The Access It! Software provides NORC with the ability to monitor Kastle card activity. The software provides administrators with the ability to review access attempts, inactive cards, and access level changes. Monthly reports used to monitor access to secure areas are reviewed by the ISO.

Zayo maintains an ERP system that collects real-time access logs for data center and secured NORC cage, which are posted to the tenant portal for review by NORC SPOCs.

The only publicly accessible area at Zayo is the lobby, which is in accessible to unauthorized users between the hours of 6:00 pm – 6:00 am. The Zayo facility does not post any exterior signage other than a small sticker on its front door. The entrance to the Zayo suite is not visible from the street.

All visitors are escorted at all times. Visitors must be escorted by an authorized tenant user at all times in the Zayo facility.

The few physical keys NORC maintains are stored in secure areas with limited access to authorized, privileged personnel. These keys unlock storage cabinets where expensive supplies, including inventoried information system components. All perimeter and restricted area doors are equipped with security card scanners.

As a tenant in the Zayo facility, NORC personnel maintain no responsibility for keys of any kind. The RFID security badges facilitate access only to areas that house NORC information systems. Within NORC facilities, NORC ISO maintains an inventory of keys, combinations and other physical access devices, which is reviewed by ISO and facilities within every 180 days.

At NORC, the AccessIt! Software maintains an inventory of active cards. Regular reviews occur to ensure inactive cards are deactivated after 90 days of inactivity. The Facilities Coordinator reviews the inventory of all badges within every 90 days.

Zayo maintains an inventory of its RFID badges in its ERP system. All RFID badges remain onsite; tenants do not remove their badges. Instead, tenants surrender a government issued ID in exchange for badge use onsite. Inventory is maintained and updated at least every 365 days.

If necessary changes to combinations and keyed locks occurs in the event of a transfer or termination. NORC retains only three sets of keys to secured systems processing rooms, which are securely stored:

- One is with the ISO Supervisor of Network Engineering;
- One is with the Director of Facilities; and
- One is held by the building landlord.

NORC has made a risk-based decision that it is unnecessary to change the keys, unless one of the holders of the keys leaves the organization, or if the key is lost or stolen.

3.7.4 PE-4 Access Control for Transmission Medium

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Protective measures are in place to control physical access to information system distribution and transmission lines which include: All cables that leave the NORC secured area at all locations are protected within conduit.

The Oak Brook, IL Zayo data center maintains the following controls of transmission medium:

- Two separate carrier node rooms are tied to distinct fiber vaults, with fiber feeds, from multiple carriers, traversing separate paths (22nd street and 294 corridor). Only Zayo staff and circuit providers have access to these rooms. Tenant cross-connect tasks are executed by Zayo staff;
- Internally, transmission medium run either overhead in mesh baskets enclosed in steel, or under the raised floor in steel conduit into each tenant’s cage and routed through cabinets in accordance with tenant requirements;
- Video surveillance covers all paths of transmission medium traversal; and
- Entry to tenant cages is restricted to authorized users only, who must use their RFID badges to gain entry to the cages.

3.7.5 PE-5 Access Control for Output Devices

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
A majority of NORC staff are field data collectors, who don’t have authorized access to facilities without escort and who do not have permissions to export data in any manner. Field laptops are locked down by security controls to prevent the external movement of data.

NORC restricts output device use for standard office users by limiting the location of NORC-owned printers, and audio devices to secured facilities. NORC prevents unauthorized personnel from having access to the output devices in NORC facilities as discussed in NORC SOPs PE-2 and PE-3. The security considerations described in NORC SOP PE-2 and PE-3 include physical authorization to NORC facilities and the physical access controls used to validate and enforce entry restrictions. Output devices are not allowed in publically accessible areas.

In addition, authorized output device users must have a charge code, which is either entered via software controls on their computers prior to printing, or via a keypad entry device on multifunction units for copying, faxing and scanning.

The NORC Rules of Behavior also address the access controls of output devices. They state that users must retrieve documents from printers immediately and must lock monitor whenever they are leaving them unattended. All NORC employees sign NORC Code of Ethics and project specific Rules of Behavior.

3.7.6 PE-6 Monitoring Physical Access, including Enhancement PE-6(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC staff monitors physical access to the building and each floor. Intrusion alarms and surveillance equipment are in place to monitor actual and potential physical access to the building after hours. Monitoring systems include surveillance of building exterior and motion-activated cameras to record activities of individuals within the facility. Physical access is monitored 24 hours a day.

Zayo's facility is protected by more advanced security controls, which are monitored by a central Network Operations Center (NOC) in the Oak Brook location, and by redundant NOCs in Zayo's other data center locations (Ashburn, VA and Denver, CO). Each Zayo NOC staffs at least two employees at all times to monitor the facility's security and automation systems. Features of the security system include:

- Entry to data center requires tenant and visitor sign in (including the surrender of a government issued ID card while on premise) at the Zayo NOC, use of RFID security badges and badge readers, biometric hand scanning, and mantraps. Additional identification validation for after-hours entry;
- A motion sensitive CCTV system covers all perimeter and internal areas of the Zayo facility (except conference rooms and restrooms) and is monitored on a 24x7 basis by the Zayo NOCs. Video footage is retained for 90 days, and can be made available to tenants upon request.

Access logs for both NORC and Zayo facilities are reviewed weekly by a Network Administrator and monthly by the ISO Director, or his designee for suspicious activities, which may include:

- accesses outside of normal work hours;
- repeated accesses to areas not normally accessed;
- accesses for unusual lengths of time; and
- out-of-sequence accesses.

The ISO Director will conduct on-demand physical access log review upon notification by Zayo of a potential unauthorized entry to the data center. Access logs associated with NORC's tenant account at Zayo are housed in the Zayo customer portal for review.

All monitoring and review efforts are coordinated with Incident Response capabilities. At NORC, off hours intrusion detection to NORC's secure facilities initiates an immediate alert to a 24-hour central monitoring service, which may result in dispatch of local law enforcement. Zayo's NOCs staff at least two NOC Engineers at all times to monitor the security of all data centers. Each data center is equipped with a NOC that is primarily responsible for its own geographical location, and provides redundant monitoring coverage for the other site locations.

3.7.7 PE-8 Access Records

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
At NORC, an electronic list of access privileges is maintained in Access It! software. Changes to this access group must be documented and approved by the appropriate supervisor.

NORC Visitors must sign login books at reception areas, which are manned by Receptionists or Security Guards. Required data elements include: date, time in, visitor name, visitor signature, organization and purpose of visit, form of ID presented, name and extension of the NORC employee being visited and time out. Depending on the building owner’s requirements, the information may be loaded to electronic systems by the Receptionist or Security Guard.

NORC generates reports of access privileges to data centers on a monthly basis which are reviewed by IT personnel, and approved by the TSS and ISO Directors.

At Zayo, visitor information is electronically entered into a Zayo portal, which is accessible to the NORC Single Point of Contact (SPOC) [role], which is served by NORC ISO Network Engineers. The SPOC requests authorization for additional NORC employees who require Zayo access to perform physical maintenance tasks to NORC’s information system. The SPOC can pull Visitor Logs from the Zayo portal. Information collected for each visitor includes: Zayo Facility (CHI-1 or CHI-2), company, visitor name, physical signature, escorted by, badge number, time in (date and time stamp), time out (date and time stamp), and notes (used for visitors who are not on the authorized tenant [including NORC] visitor list).

Authorized tenant users also provide a secure password with Zayo, which must be provided to gain entry after standard hours.

All physical access logs are retained for seven years.

Visitor access logs are maintained and reviewed monthly by Security Guards. NORC generates reports of access privileges to data centers on a monthly basis which are reviewed by IT personnel, and approved by the TSS and ISO Directors.

Zayo’s visitor records for NORC are posted to the Zayo portal for review by NORC ISO Engineers who serve as NORC’s Single Point of Contact (SPOC) role at Zayo.

3.7.8 PE-9 Power Equipment and Cabling

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC maintains power equipment in secure monitored locations. Main power equipment for NORC facilities is maintained in maintenance rooms only accessible by authorized NORC personnel and building management. NORC facilities have power equipment and distribution for information system components secured by physical security controls. Access to the NORC server room power equipment and cabling is further restricted by keycard access to the NORC Engineering Team.

The Oak Brook, IL Zayo data center facility maintains the following security controls to protect power equipment and power cabling:

- Electrical circuits are routed under raised floors in dedicated conduit. All electrical feeds run through zone specific UPS and line conditioners to provide constant power feeds at appropriate voltage levels;
- A & B circuit outlets are routed into locking outlets under-cabinet spaces and protected by airtight jacketed boots, to

prevent dust, debris or water from interfering with power delivery;

- Generators are protected from unauthorized tampering by security walls;
- Access to electrical service and UPS rooms is limited to Zayo Electrical Engineers and NOC personnel;
- All areas of electrical circuit traversal are monitored by motion-sensitive CCTV cameras, with footage retention of 90 days; and
- Power distribution units, which contain circuit breakers are housed adjacent to tenant cages.

3.7.9 PE-10 Emergency Shutoff

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
An emergency shutoff in the NORC server room is available to cut power to all information system hardware. Testing of this capability has occurred. Zayo data centers are equipped with Emergency Power Shut Off switches adjacent to ingress/egress points. These are dual press buttons, each protected by separate covers.

The emergency shutoff switch is available in the NORC server room. Authorized personnel maintain access to this room. At Zayo, emergency power shutoff switches are located on walls adjacent to ingress/egress points.

The emergency shutoff is located in the secure NORC server room. Limited authorized access is provided to this room. It's protected by the RFID AccessIt! card access it system. At Zayo, the act of raising the covers triggers an alarm in the Zayo NOC. These switches are monitored by CCTV cameras, so in the event of an unauthorized, or unnecessary, shut down of power, the responsible person can be identified.

3.7.10 PE-11 Emergency Power

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC Data Centers - An uninterruptible emergency power is provided by NORC. The emergency power system provides medium-term, uninterruptible power to all critical IT systems stored in the NORC Data Center. This system is fully tested once a year and some components are tested more frequently.

Zayo Data Center - All data centers are protected by A & B electric generator feeds with additional swing generators, with automated transfer switches that can detect primary generator failures, and migrate to alternate feeds to facilitate uninterrupted service. Generators are protected from unauthorized tampering by security walls.

A & B circuit outlets are routed into locking outlets under-cabinet spaces and protected by airtight jacketed boots, to prevent dust, debris or water from interfering with power delivery.

Access to electrical service and UPS rooms is limited to Zayo Electrical Engineers and NOC personnel.

Power distribution units, which contain circuit breakers are housed adjacent to tenant cages.

Each generator is capable of producing 1.25 megawatts of power, and at full load can run for 48 hours before it must be refueled. In practice, since load is balanced by at least two generators, run time should extend to 72 hours. Zayo's total generator power load is 24 megawatts.

Zayo Facilities Engineers cycle and test each diesel generator at least weekly in warm months and twice weekly in cold months, and conduct semi-annual full-load tests. Two Facilities Engineers and at least 1 NOC Engineer participate in the tests, and four distinct sign-offs for each test validate the results.

The Oak Brook Zayo facility houses State of Illinois disaster recovery equipment. As a critical component of the state's infrastructure, Zayo maintains premier filling rights.

3.7.11 PE-12 Emergency Lighting

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC provides emergency lighting to facilitate an orderly evacuation of the facilities in the event of a primary power source loss, illuminating exits and evacuation routes throughout the facilities. NORC data centers are equipped with automatic emergency lighting that activates in the event of a power outage or disruption.

At Zayo, emergency lighting illuminates all areas of egress including regular and emergency exits, as mandated by the Village of Oak Brook and in compliance with Chicago Fire Code standards. Emergency lighting is tested on a semi-annual basis by Zayo facilities engineers and the Oak Brook Fire Department.

3.7.12 PE-13 Fire Protection, including Enhancement PE-13(3)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Zayo's fire detection and suppression systems are continuously monitored and tested semi-annually by the Zayo NOC and Facilities Engineers, with the cooperation of the Oak Brook, IL Fire Department. The system is architected to detect the presence of smoke early, so NOC personnel can respond prior to a fire actually breaking out. The system is powered by utility power, but cuts over to generator power in the event of a power interruption. Fire extinguishers are located every 500 feet throughout the facility that may be used to choke an isolated fire. The facility is monitored by a CCTV camera system, so that if the fire alarms are set off inappropriately, Zayo Engineers can detect the source.

3.7.13 PE-14 Temperature and Humidity Controls

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Liebert unit controls temperature and humidity to all areas of the NORC server rooms with alarms set if levels are out of tolerance. Each server cabinet has its own alarm for this purpose.

Acceptable environmental levels before alerts are sent out to staff:
Temp: Set point = 68°, Hi = 80°, Lo = 60°
Humidity: Set point = 20%, Hi = 75%, Lo = 15%

At Zayo, temperature and humidity controls are managed in accordance with ASHRAE 2011 standards. Alerts are generated for NOC Engineers and designated NORC personnel, when readings exceed the upper and lower thresholds.
Temperature set point = 70°
Allowable temperature range = 59° - 90°
Allowable humidity range = 20% - 80%

In the event of a power disruption, generators will power HVAC units. Zayo NOC operations continuously monitor temperature and humidity controls.

3.7.14 PE-15 Water Damage Protection

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
In the NORC data center, water sensors are in place under the raised floor of the server room.

Equipment used to monitor environmental controls is secured in the Zayo NOC at each location to keep the equipment safe. Water detection and temperature sensors are present in drip pans underneath HVAC units, and adjacent to drip pans under the raised floors. Water detection sensors are tied into the facility’s building automation system. Presence of water may trigger cut over to generator power.

Zayo NOC Engineers have been trained to protect the data centers from water damage, by turning off the water to the facility at the main water shutoff valves.

3.7.15 PE-16 Delivery and Removal

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Equipment is installed by approved NORC staff with the exception of mechanical systems, which require approved NORC staff presence for installation. NORC must authorize, monitor, and control selected information system components entering and exiting NORC facilities and must maintain records of those items. Chain of custody controls exist from the time the package enters the facility until it is installed or otherwise put into production.

At Zayo:
Shipping – NORC must initiate coordination with the Zayo NOC by submitting a ticket through the Zayo customer portal. NORC must arrange for the courier pickup and provide the Zayo NOC with the fully addressed package with the courier slips completed. All shipping costs are attributable to NORC, and courier account numbers must be NORC’s. Packages must be delivered to the Zayo NOC, whose personnel will take the packages to a secure shipping/receiving suite. Couriers pick up

packages from this secure location.

Receiving - Tenants may receive deliveries at the Zayo data center(s), but they must first authorize the deliveries via a ticket in the Zayo portal. Strict chain of custody protocols are attached to the ticket:

- Zayo applies barcodes to packages upon receipt at the facility for tracking in the portal.
- Zayo will store a package for up to three weeks without charge to the tenant. Storage after three weeks is a chargeable event to the tenant.
- Tenants must electronically sign for the package upon turnover, which is added to the ticket prior to close out.

All delivery and removal of hardware is documented in a hardware tracking system as well as the change management system.

3.7.16 PE-17 Alternate Work Site

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC maintains multiple offices across the country. If one work site is unavailable, the first option would be to redirect work to another office, particularly, Precision Opinion’s Las Vegas call center facility. However, if a work site may become unavailable for an extended period of time, NORC may allow employees and contractors to work from home, provided they follow defined security guidelines and acceptable usage rules applicable to all people and information systems.

NORC maintains physical and environmental protections at alternate work sites, which include fire detection and prevention, temperature and humidity controls, use of RFID badges for areas other than publicly accessible space, and monitoring of equipment delivery and removal.

Privileged users may work from their private residences if they have been authorized for remote access. Private residences will only be used in the context of remote access/telework, or in the event of an unforeseen contingency or disaster scenario, in which a NORC facility is unavailable. NORC follows the guidelines from NIST Special Publication 800-46 to govern use of systems from private residences. Systems used at the residences of employees must be organizationally owned and controlled, encrypted to protect data at rest, and access to NORC systems is limited.

Systems at alternate work sites check in with NORC’s System Center Configuration Manager (SCCM), which is used to monitor and assess the effectiveness of Mobile Device security controls.

When an alternate work site is in use, personnel may continue to use resources made available for information security assistance. These include the NORC ticketing system, the ir@norc.org incident email address, and security guidelines provided on the NORC Intranet site.

3.8 Personnel Security (PS) Controls

3.8.1 PS-1 Personnel Security Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC Security, Personal Security Policy, is the formal, documented personal security policy and addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities/personnel (i.e., the system administrators, ISSOs, system owners/business owner, and users etc.), and compliance.

The NORC Security, Personal Security Procedures, contains documented procedures to facilitate the implementation of the personal security policy and associated controls.

Continuous Monitoring – NORC reviews organization-wide policies and procedures annually, which NORC defines as within every 365 days. If any changes are made, NORC policy and procedures are adjusted accordingly.

3.8.2 PS-2 Position Risk Designation

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
All NORC organizational positions require a job description which includes consideration for risk surrounding the positions responsibilities. All NORC positions are designated with either a High or Moderate risk, given the access to PII on project work.

Job applicants are assessed by comparing the applicant’s skills (e.g. communication skills, computer skills etc.) and traits, against minimum and specific, position requirements. Specific screening and background investigations are determined by role, and in accordance with organizationally-designated risk profile(s). NORC employees may be subject to additional screening as roles change and project or departmental requirements dictate. NORC employees are aware of these conditions through the NORC policy, “B2 – Background Investigations,” which is published on the policy portal of the NORC InSite intranet.

Human Resources reviews the risk designations by role and the screening criteria every 365 days, or when there is a change in the responsibilities of the position or of the information or facilities which must be accessed to perform the duties of the position, whichever is sooner.

3.8.3 PS-3 Personnel Screening

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC Background Investigation (BI) Release Form(s) are completed by applicants and authorize NORC Human Resources staff to process BI’s on employees depending on the function of the position for which the applicant is being considered.

Projects requiring periodic re-screens are typically dictated by federal agency clients, and NORC HR facilitates background investigations accordingly.

3.8.4 PS-4 Personnel Termination

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Upon termination of individual employment or contract, NORC revokes information system access. NORC ISO Administrators revoke information system access for an individual as directed by HR and management. An individual's access is revoked COB of a standard termination; access is disabled immediately for a hostile termination event.

Access removal consists of the following procedures:, Disabling the user account in Active Directory, Revoking any user certificates, and Removing the user's access card privileges

NORC is required to conduct exit interviews when possible. As part of NORC's termination procedures, NORC HR conducts exit interviews of outgoing personnel, which includes the following information security content:

- Collection of NORC information systems property and physical security badges,
- Reminder of any Non-Disclosure Agreements, Rules of Behavior forms and other project-specific confidentiality documents that the employee may have signed, along with the obligations and legal requirements associated with the executed commitment: and
- Notification that all access to information systems will be revoked immediately.

NORC collects all security related organization information system property at the exit interview. Managers are directed to also collect their terminated employees Access Card, physical access keys if applicable, and laptop and mobile devices.

While the individual's access will be removed by disabling their account, NORC will retain access to organizational information and information systems formerly controlled by the terminated individual.

NORC ISO Administrators revoke information system access for an individual as directed by HR and management.

3.8.5 PS-5 Personnel Transfer

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization.

NORC TSS initiates reassignment of privileges within 24 hours of departmental transfer notification. Transferred personnel are reassigned access privileges in accordance with the principle of least privilege. Formal transfer actions to be executed by TSS/ISO include: token provisioning and/or swaps, physical access grants or revocations, Access Control List changes, Account provisioning or revocation, addition to or removal from security groups, and network access changes.

When assigning new privileges and evaluating pre-existing privileges of transferring personnel, NORC uses the concept of least privilege.

Notifies TSS Helpdesk within 5 days of the formal transfer action.

3.8.6 PS-6 Access Agreements

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC ensures that individuals requiring access to NORC information systems and data sign the appropriate access agreements prior to being granted access. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized.

NORC maintains an internal tracking system which is used to track and verify that agreements have been signed per individual. NORC may require employees and contractors to re-sign access agreements, in accordance with the frequency requirements of each project as mandated by the sponsoring agency requirements.

NORC Project Teams reviews and updates the access agreements on an annual basis, defined by NORC as within every 365 days. NORC Project Teams may be required to review access agreements more often based on contract.

3.8.7 PS-7 Third-Party Personnel Security

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC limits third-party interactions with NORC information systems. Third- party personnel are granted only limited roles and responsibilities in regard to NORC information system components.

NORC requires third-party personnel to complete the following security requirements before interacting with NORC information systems: Complete the Security, Role Based and Project specified training Sign the NORC Statement of Ethics, Data Use (DUA) and Confidentiality Agreements.

Documentation of NORC security requirements must be submitted to NORC Human Resources, Project Directors and Management before access is granted to NORC information systems.

Requires third-party providers to notify responsible NORC manager(s) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within the same day of personnel change.

NORC monitors provider compliance through the use of onsite managers. NORC requires onsite managers to notify NORC of all personnel changes including employment, transfers, and termination. Onsite managers also report to NORC on the status of security requirements and provide evidence of completion. NORC maintains documentation of security requirement fulfilment.

3.8.8 PS-8 Personnel Sanctions

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Verbal and written warnings are employed for minor incidents. Penalties are in place up to criminal prosecution and termination. All incidents are documented.

Managers notify the Human Resources and the TSS Helpdesk to alter access privileges within one day when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. The topic of personnel sanctions is addressed in the NORC HR Policy, C5-“Discipline”, which is distributed to employees upon hire and is located in the Policy Toolkit, posted on the NORC InSite intranet portal.

3.9 System and Information Integrity (SI) Controls

3.9.1 SI-1 System and Information Integrity Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “System & Information Integrity Policy” which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to System & Information Integrity.

The NORC Security, System and Information Procedures, contains documented procedures to facilitate the implementation of the System and Information policy and associated System and Information controls.

Continuous Monitoring – NORC reviews organization-wide policies and procedures at least annually, which NORC defines as within 365 days. If any changes are made, NORC policy and procedures are adjusted accordingly.

3.9.2 SI-2 Flaw Remediation, including Enhancement SI-2(2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC identifies information system Components containing software affected by announced software flaws and reports this information to designated personnel responsible for the affected system component. NORC monitors public vulnerability databases and vendor provided vulnerability lists for software and hardware flaws and vulnerabilities that may have an effect on NORC information systems.

Based on device, NORC implements specific procedures to ensure the software or firmware is tested prior to live implementation.

Windows servers are patched the second Tuesday of every month. Patches are applied within 30 days of release of updates. Network devices vary because of the severity of the implementation, devices affected, and other factors.

NORC uses the Shavlik system to determine the status of patch deployments on Windows Systems. Shavlik repost missing patches and any errors related to patching systems. At a minimum, NORC scans monthly with automated NESSUS Enterprise system for all NORC servers. NORC audits Systems on a monthly basis for industry vulnerabilities, vulnerabilities in standard system assets and applications, and missing patches.

3.9.3 SI-3 Malicious Code Protection, including Enhancements SI-3(1) (2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The organization centrally deploys and maintains malicious code protection software capable of remote updates including McAfee’s enterprise package. Barracuda provides SPAM and Spyware protection for email communications. NORC centrally manages virus protection mechanisms. Virus signatures and updates are scheduled and sent out to systems every 4 hours, ePO software is updated annually per vendor notification.

Virus protection software is managed by a client/server application. The virus scan management server downloads new virus signatures and scanning engine updates from the vendor as they become available. The new virus signatures and updates are then pulled from the virus scan management server by the client software located on workstations and servers. This process is generally scheduled to take place every 4 hours.

The client software has been configured to perform the virus scanning function every four hours and reports the scan status back to the virus scanning management server. All workstations are set up with virus scanning client upon creation. Most servers are set up with virus scanning software as the software system allows. Additional real-time malicious code scanning is provided by core network firewalls and the Spam and Virus Firewall as files are downloaded, opened or executed. Malicious code is blocked and an alert of the presence of malicious code is sent to eIQ SecureView, which alerts the ISO Director and key ISO Engineers.

The configuration of malicious code protection mechanisms is reviewed and adjusted on a continuing basis in order to provide maximum protection while reducing the number of false detections issued by the mechanism.

3.9.4 SI-4 Information System Monitoring, including Enhancements SI-4(2) (4) (5)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC employs automated system auditing tools (Varonis, Idera) and manual system auditing techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

NORC identifies unauthorized use of the information system through automated monitoring tools and unauthorized access attempt alerts to ISO Engineering personnel.

What’s Up Gold monitors all server activity, and Idera monitoring tool is deployed for all production databases. NORC employs automated tools SecureVue eIQ Log Management System (LMS) SIEM, Varonis and McAfee ePolicy Orchestrator (ePO) to assist with incident identification. The Zayo ERP system, with customer interaction portal, provides real-time monitoring of entry into the secure data centers where NORC information systems are housed, including entry into NORC’s private cages. Incident response team members are automatically notified and alerted when incidents occur.

Access to NORC devices and software carrying out intrusion detection and prevention functions is restricted to NORC System Administrators with privileged accounts. eiQ, Varonis and Idera tools do not allow undetected changes to the records by NORC System Administrators. Alerts are setup to monitor these tools internal data changes.

NORC heightens the level of information system monitoring activities 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.

NORC obtains legal opinion from NORC’s Contract and Legal department with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

NORC information system must provide near real-time alerts to the ISO Director and ISO Engineering Team when any of the following indications of compromise or potential compromise occur: Malicious code is detected, Denial of Service Conditions, System or Service unavailability, Network device configuration changes, and Physical intrusion\Environmental impact.

NORC employs multiple tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. What’s Up Gold provides these protections for the network. Idera Compliance and Security software provides protection for NORC’s databases. EIQ SecureView monitors system access and alerts the appropriate personnel for failed logins and excessive successful logins.

This continuous monitoring is accomplished with the Juniper VPN and Cisco firewall devices. Connection logs on individual system components are sent as syslogs to the eiQ Log Management System. NORC utilizes the McAfee Enterprise Virusscan/Anti-spyware products to monitor inbound and out bound traffic communications for unusual or unauthorized activities or conditions.

NORC information system must provide near real-time alerts to ISO Security personnel when any of the following indications of compromise or potential compromise occur: Malicious code is detected, Denial of Service Conditions, System or Service unavailability, Network device configuration changes, and Physical intrusion\Environmental impact.

3.9.5 SI-5 Security Alerts, Advisories, and Directives

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC receives information system security alerts, advisories and directives from US-CERT, SANS, SearchSecurity, SecurityFocus-Bugtraq and system vendors.

The NORC ISO and TSS Directors, as well as the Chief Privacy Officer may generate internal security alerts, advisories and directives, via email or Intranet publishing, to NORC personnel to ensure wide-ranging knowledge of the organization with respect to current information security risks and best practice guidance.

The ISO Director (CISO) and the IT Security Compliance Supervisor forward applicable materials to ISO Engineers and TSS personnel (who hold configuration/patch management responsibilities) to facilitate information sharing in support of maintaining a strong awareness of potential security risks and best practice guidance.

NORC implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

3.9.6 SI-7 Software and Information Integrity, including Enhancements SI-7(1) (7)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC employs integrity verification through a series of applications and hardware that include:

- Microsoft Windows System File Check (SFC) and Linux File Scanning Check (fsck) – upon security update installation / patch application and after a reboot caused by a system failure
- Firmware / BIOS Update Integrity Checking – upon security update installation / patch application and after a reboot caused by a system failure
- McAfee Anti-virus and Anti-Spyware software – upon download of policy update and when a virus is detected
- Barracuda SPAM and anti-virus firewall for NORC email systems – when firmware upgrades are readied for implementation, upon receipt of external emails.
- Intrusion Detection System (IDS) on the Cisco ASA network firewalls – continuous monitoring of network traffic

- Varonis DatAdvantage – reports on changes to file server data (authorized or unauthorized)
- Shavlik NetChk Protect patch management for all Windows machines and a subset of NORC Enterprise applications – upon command to apply patches to servers
- eIQ Audit Log and configuration monitoring and reporting to alert administrators of changes in NORC servers – monitors hosts for abnormal events
- Weekly Monthly Nessus scans – after server installation and prior to implementation; weekly vulnerability scans of servers
- WinMagic HDE integrity checking – at bootup of PCs

Detection of security-relevant events, including unauthorized changes to the information system must be tracked, monitored, corrected and available for historical purposes. These incidents must be managed in accordance with the protocols and processes defined in the NORC Incident Response Plan.

3.9.7 SI-8 Spam Protection, including Enhancements SI-8(1) (2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC employs and centrally manages spam protection via the Barracuda Spam & Virus Firewall that is used as a relay into our Microsoft Exchange email server environment. This appliance scans all incoming and outgoing email and email attachments for spam and viruses.

Barracuda automatically updates spam and virus definition signatures daily during an automated process carried out by the system. Updates are made to the firmware as they become available.

3.9.8 SI-10 Information Input Validation

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC ensures that vendor provided components of NORC information systems employ technical controls that check input for valid syntax and semantics. For NORC developed software, NORC employs input validation.

Case files are encrypted with 128 bit encryption during transfer from data collection to database upload. Hashes of zip files in transit can be examined if decryption problems occur, indicating that the file may be corrupted.

Data validation occurs via post processing to ensure integrity. Back-up files are made at all stages to recover data and perform further data integrity analysis.

3.9.9 SI-11 Error Handling

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC systems log system errors. Users report any system errors to the Help Desk team. All application log files are written to a secure network area which only authorized personnel have access to. The groups of users with access to the application logs are application developers, network engineers and help desk staff.

3.9.10 SI-12 Information Output Handling and Retention

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The systems handle and retain output from the information system in accordance with Agency and system-specific requirements. Data is handled, retained and maintained with record retention guidance due to its longitudinal nature. Procedures are in place to protect and safeguard against any potential disclosure of sensitive information.

3.9.11 SI-16 Memory Protection

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC IT utilizes multiple controls to protect its information systems component memory from unauthorized code execution.
System Administrators rely on standard memory protection controls in Windows and Linux. Servers are configured to prevent hardware-based data execution by default. Virtual memory on servers is dumped upon restore.

Application Development codes in object oriented languages, which take advantage of sandboxes, virtual machines and garbage collectors to manage memory, ensuring that code is only executed in authorized memory spaces, and cleared upon completion of the code functions. Thorough testing in test environments prior to release validates proper security controls and business functionality.

McAfee VirusScan and AntiSpyware Enterprise software protects systems against malware threats. Firewalls, IDS/IPS and other filtering devices monitor traffic and send alerts to Network Engineers, who will respond to threats of attack that might compromise information systems.

4.0 TECHNICAL CONTROLS

4.1 Access Control (AC) Controls

4.1.1 AC-1 Access Control Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled "Access Control Policy" which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Access Control..

The NORC security policy Access Control Procedures contains documented procedures to facilitate the implementation of the access control policy and associated access control controls.

Continuous monitoring –NORC reviews organization-wide policies and procedures annually as defined within every 365 Days. If any changes are made, NORC policy and procedures are adjusted accordingly.

4.1.2 AC-2 Account Management, including Enhancements AC-2(1) (2) (3) (4)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
A. NORC employs automated mechanisms to support the management of information system accounts by using Microsoft Active Directory (AD) for IT systems account management. Active Directory employs RBAC and dynamically manages user privileges and associated access authorizations. Access privileges are determined and granted based on valid access authorizations, intended system usage, and other attributes of the Organization or associated Mission or Business functions.

B. NORC establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles. The NORC IT Department utilizes an interface between Varonis and Microsoft AD for the automated provisioning of project data access permissions, following the Information Owner's authorization of a user access request.

C. Group membership is determined by the user's role within the Organization and the mission area or business function they perform.

D. The NORC IT Department is responsible for performing the following account actions relative to account management: Establishing accounts, Activating accounts, Modifying accounts, and Disabling accounts.

E. NORC IT requires appropriate approvals for requests to establish accounts. An in-depth process that covers account establishment, activation, modifications, disablement, and removal can be found in NORC IT Standard Operating Procedure IT-01 (AC-2) Account Management.

F. When an employee or contractor separates from NORC their accounts are immediately disabled. Notification goes through our HR process to remove the account and all associated reference access in active directory. Accounts are monitored on at least a 6 month basis either through generation of a report for all system specific associated AD groups by project or through web interface using NETIQ tool.

G. NORC tracks and monitors privileged role assignments. Varonis software assists management with monitoring account access attempts. NORC monitors information systems for atypical usage, especially during hours of system inactivity. Any atypical usage of information system accounts is investigated by ISO Staff and reported appropriately to designated, NORC ISO Management. All account management activities are logged on the account management systems. In addition, are logged on the account management systems In addition, these SIEM logs are gathered by a centralized SecureVue IQ log management system (LMS). The LMS is capable of alerting account and system managers of any account related activities.

H. In the case of involuntary separation of an employee, such as termination, the IT Department is notified ahead of time or in the case if the termination is of an immediate nature. A formal notification process exists when employees voluntarily separate from NORC.

I. NORC IT requires appropriate approvals for requests to establish accounts. An in-depth process that covers account establishment, activation, modifications, disablement, and removal can be found in NORC IT Standard Operating Procedure IT-10 - Account Requests.

J. NORC TSS Level III Representatives review accounts after account creation and prior to account enablement for accuracy and adherence to standard account attribute conventions. ISO and TSS Engineers periodically, but no less than annually, run Varonis DatAdvantage reports to audit accounts in Microsoft Active Directory to review access privileges and review the following account actions:

- Account creation
- Account modifications
- Disabling of accounts
- Account terminations

K. A set security groups is created to provide access to a single resource. Each resource has a unique set of groups each granting a level of access including read, modify and full. Group membership is dictated by the resources an account is authorized to access. The authorization is provided by the data or system owner, or their delegate. Each user has at least one unique account. This account is used to grant access to NORC resources. When a new account is requested or a change to an account is requested, a tracking ticket is created by the Help Desk personnel to document the data to be accessed, the required access level, and approvals necessary to grant access. Once approval is granted, systems administrators provide the necessary accounts or make the necessary changes.

Access to project data is authorized by NORC Information Owners. The provisioning process of the access is an automated project via Varonis interface to Microsoft Active Directory. End users requiring access to project folders within the norc.org domain go to the Data Privilege site at http://access.norc.org, where they complete the “Permissions Request” form. The submission of the form triggers an automated e-mail to the Authorizers/Approvers of the project folder group. The Authorizer responds to the email using radio buttons to indicate a decision to 'Approve' or 'Decline' the request, along with a typed explanation for the decision. Notification of the decision is e-mailed to all Stakeholders. If the request is approved, Varonis scripts send the access information to Microsoft Active Directory, which updates the user access privileges.

Temporary account access must be specifically authorized and monitored. Temporary access may be granted in very rare cases where system access is required for systems maintenance (i.e. emergencies) or to fulfill pertinent mission or business functions and those accounts are audited closely.

Built-in Guest and Anonymous accounts are not used for temporary or emergency access. Rather, the authorized individual(s) are assigned a regular account for a certain amount of time. Temporary and emergency accounts are automatically set to be disabled at the end of individual's last day worked. In cases where a temporary account is established and the last day of work is unknown, NORC will notify account managers when temporary individual accounts are no longer required and those accounts will be disabled.

NORC employs Netwrix software that automatically disables inactive accounts. An Inactive account is any account that has not contacted the account management system in 60 days. NORC automatically disables accounts which have been inactive for 60 days.

NORC monitors information systems for atypical usage, especially during hours of system inactivity. Any atypical usage of information system accounts is investigated by ISO Staff and reported appropriately to designated, NORC ISO Management. Removal of system accounts is a manual process that is executed by TSS staff after management authorization decisions.

4.1.3 AC-3 Access Enforcement

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC information systems enforce Role-Based Access Control (RBAC) where the Policy establishes coverage over all users and resources to ensure that access rights are grouped by Active Directory role name, and access to resources is restricted to users who have been authorized to assume the associated role.

Information Owners (Business Project Leads) determine the groups and access privileges appropriate for each employee. Access privileges are granted by the System Administrators, or by automated mechanisms, only after access authorization, Permissions are reviewed periodically by Information Owners and IT Management in accordance with Risk Assessment procedures.

4.1.4 AC-4 Information Flow Enforcement

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Policy for controlling the flow of information within systems and between designated source and destinations is based on the defined system boundaries, business needs, and applicable policies as well the characteristics of the information or information path. A secure FTP server controls information flow and maintains encrypted communication of respondent and systems data. Internal flow control is enforced through the presence of proper rule sets on firewalls. Firewall rule sets are audited quarterly. The firewall rules blocks all external traffic that uses NORC internal addresses or RFC 1918 private address space. NORC blocks all inbound traffic from session initiation with any internal devices. NORC limits all outbound traffic to only known protocol ports.

4.1.5 AC-5 Separation of Duties

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC employs a change management system that prohibits unilateral system changes. A control board meets weekly to approve non-emergency changes. Specific units within the NORC information technology department separates IT responsibilities.

Procedures are in place to note that checks and balances must be present for all access controls. Documented Separation of Duties (SOD) is found in NORC IT-03 SOD SOP.

4.1.6 AC-6 Least Privilege, including Enhancements AC-6(1) (2) (5) (9) (10)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Privileges are designated by role. NORC systems are divided into subnets. Also roles are technically enforced to prohibit unilateral action. NORC employs the concept of Least Privilege on its networks, allowing only authorized access to users necessary to accomplish tasks in accordance with organizational missions and according to their job roles. All IT Engineering, Network Services, and Technical Support Services (TSS) staff have access to various security functions employed within hardware, software and firmware and only personnel with roles associated with those security functions are granted explicit access to correlating technologies. All new NORC employees or contractors who go through hire process are granted minimal access privileges to the NORC network. Users are only granted access to resources as needed at the lowest level of access to do their jobs and/or based on their Department Head or Managers approval.

Remote data collectors are restricted by a locked down configuration that only permits limited actions. Other remote users are restricted by subnets and SSL VPN and Citrix.

By default only system administrators have administrative access to NORC systems. Only service accounts and system administrators have direct access to production systems.

Users of IT System accounts or roles with access to security functions or information use non-privileged accounts of roles when accessing other IT Systems functions. Administrator account usernames are clearly demarcated from their non-privileged accounts by inclusion of the term “admin.” The non-privileged naming convention for a NORC user account is ‘last_name-first_name’. An admin account’s naming convention is ‘last_name-admin’. A third category for application administrators, who have limited privileges is indicated by an account naming convention ‘last_name-priv’.

Non-administrative support personnel are given minimal access (Read-Only) to production systems logs and other outputs.

NORC audits privileged accounts, and/or roles with access to security functions or information use non-privileged accounts of roles when accessing other IT Systems functions.

Information systems privileges are configured by group policies. Only privileges users are provisioned with access to execute privileged functions, in accordance with the responsibilities for their jobs. Further delineation of privileged functions, in accordance with segregation of duties and least privilege controls, prevents cross-functional execution of activities. For instance, Server Administrators can alter security configurations on servers, but they do not have access to make switch, router or firewall configuration changes. Help desk support personnel may hold greater privileges than end users, but they are unable to administer server administration changes or circumvent security configurations that have been administered.

4.1.7 AC-7 Unsuccessful Logon Attempts

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The OS enforces a limit of three consecutive invalid access attempts by a user. NORC follows the Center for Internet Security (CIS) Standard:

1. Account Lockout Duration:	15 minutes
2. Account Lockout Threshold:	3 attempts/15 minutes
3. Reset Account Lockout After:	15 minutes

4.1.8 AC-8 System Use Notification

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Users are notified that they are utilizing NORC systems with access to government-owned data. The logon banner, see below verbiage, is presented to all internal users at the windows login and to external users which include all same warnings as a government system user.

THIS IS A PRIVATE COMPUTER SYSTEM!

This computer system is for official NORC use only. Unauthorized use is prohibited. NORC routinely monitors the use of our computers and may record the results of our monitoring for legal or disciplinary action. By accessing this system, you agree to these terms. If you are not authorized to use this system, exit immediately.

NORC operates and manages Information Systems and Data for the U.S. Government and other agencies, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. Unauthorized use of these systems or unauthorized access to data to which you have not been granted explicit authority to utilize is a violation of Federal Law and subject to criminal and civil penalties including fines and imprisonment (Public Law 99-474). Use of these systems indicates consent to monitoring and recording.

The user is presented with the login banner and either hits the “Enter” key or clicks the “Accept” button to signify acceptance of the login banner terms and conditions

4.1.9 AC-11 Session Lock, including Enhancement AC-11(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
All devices on the network capable of implementing password-protected screen savers implement this feature with a maximum inactivity time of fifteen (15) minutes.

The password-protected screen savers require the user to reestablish their identity using appropriate identification and authentication procedures. A password-protected screen saver is implemented with a maximum inactivity time of fifteen (15) minutes to conceal publicly viewable images.

4.1.10 AC-12 Session Termination

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC configures session termination settings at the application-level for non-privileged users. After 30 minutes of inactivity, applications user drop sessions, forcing users to log in to create new sessions.

Some privileged users, who execute privileged functions may be configured to bypass the session termination restrictions, as their functions may take longer than 30 minutes to process. The sessions are protected by session lock, as defined in control AC-11.

4.1.11 AC-14 Permitted Actions Without Identification or Authentication

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC does not permit any actions without identification and authentication. All NORC users are required to have a unique identifier that is used in the authentication process granting them access to a system. As such, no anonymous access is permitted. ISO Engineers apply OS level configuration settings in accordance with CIS benchmarks to prevent anonymous activity within the NORC information systems environment.

Procedures are in place to for the user actions that are performed on the information system without identification or authentication as documented in our domain group policies and IT-57 Permitted Actions Without Identification and Authentication SOP.

4.1.12 AC-17 Remote Access, including Enhancements AC-17(1) (2) (3) (4)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Per NIST supplemental guidance, NORC maintains remote connections via VPN and we treat these connections as internal because effective security controls have been applied. Controls are listed below:

The identity of remote users must be challenged and validated prior to allowing access to NORC resources. A second login is required for access to data collection resources. Two factor authentication is used for remote access using a software certificate and AD credentials.

Security parameters for remote access points of entry must be easily configured and verifiable from the central network management facility. Locked down laptop configurations are in place for data collectors that restrict users to remote desktop and VPN privileges. Locked down laptop configurations using USGCB are in place for data collectors that restrict users to remote desktop and Juniper VPN privileges.

NORC documents allowed methods of remote access to the information system and establishes usage restrictions and implementation guidance for each allowed remote access method. Additionally:

+ All remote access is logged in the Juniper appliance and also sent to the EIQ Security log monitor to ensure compliance.
+ The Juniper VPN concentrator is certified FIPS 140-2 compliant. All session traffic is encrypted to ensure confidentiality and integrity of the session.
+ All remote access is controlled through a pair of Juniper VPN concentrators. This is the only remote access method allowed within NORC.
+ The access to privilege commands and security related information are limited to the ISO group. This group must have it to maintain the continued operations of the NORC infrastructure.
+ NORC uses EIQ to monitor for unauthorized access to information systems and takes the appropriate actions as necessary.
+ All remote access sessions must use two-factor authentication. In addition to their active directory id and password, the user must have a digital certificate installed on the machine.

NORC restricts the use of privileged commands or access to security-relevant information via remote access methods to authorized IT employees, who require this level of access to support the information system.

In the case privileged commands or access to security-relevant information access is required by contract, the requirements, compelling business need, and appropriate compensating controls are documented in the system security plan.

4.1.13 AC-18 Wireless Access, including Enhancement AC-18(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has implemented three types of access restrictions to its WLAN as follows:

Guest - Guest access only allows Internet connectivity. The connectivity is on a separate segment that does not communicate to the NORC secure network. Guest devices obtain DHCP from the wireless domain controllers and are then placed in a tunnel. The terminating tunnel endpoint is the controller that connects directly to the Internet firewall.

Bring-Your-Own-Device (BYOD) – BYOD devices obtain limited access to NORC resources. BYOD devices are allowed this type of connectivity only if the user has an Active Directory (AD) account in the NORC private network. BYOD devices are only allowed specific resources that are web browser-based. The BYOD device is not allowed access to any project or sensitive data

NORC Employee Access - Employee access is allowed with only NORC laptops that have the required antivirus and security configurations implemented. The devices must be recognized by the AD domain controllers and the end-user must have an account on the NORC private network. If the device is recognized by the domain controller and the user is not recognized, the device will be placed on the Internet segment (BYOD). The wireless card is disabled on project laptops that are not allowed to use wireless access. There are no wireless cards on desktops or servers.

Guests must obtain an SSID password from a sponsor. Credentials are verified by the NORC AD domain controller.   NORC has implemented WPA2, Pre-shared Key (PSK) network authentication with AES encryption for guest SSID access.

Wireless emanations are also controlled The Aruba wireless system is configured to identify and alert in the event of a rogue device that is attempting to take over the NORC wireless airspace. NORC has configured the wireless system to alert of a rogue device if that device is attempting to spoof an Aruba access point. The Aruba controller is configured to “fingerprint” the airspace where an Aruba access point is installed. The Aruba controller is configured to alert when an unauthorized device is trying to use the NORC SSID.

NORC has implemented WPA2 network authentication AES encryption on the NORC-Secure SSID access. The end device must have WiFi-Protected Access Generation 2 (WPA-2) network authentication, Advance Encryption Standard (AES) encryption, Protected Extensible Authentication Protocol (PEAP) with an Addtrust External Certificate Authority (CA) Root enabled, and user or computer authentication mode enabled.

4.1.14 AC-19 Access Control for Mobile Devices, including Enhancement AC-19(5)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
For corporate employees, TSS installs Good Mobile Messaging on smartphones, which provides an encrypted container for NORC email. Good allows TSS to monitor the location of smartphones. TSS can remotely wipe the contents of the Good application, in the event the employee loses the smartphone.
Field Interviewers use NORC-owned smartphones and tablets as data collection devices. TSS installs Airwatch as a primary component of the device configuration, which allows TSS to remotely manage patches, control data storage, email, encryption, and enterprise architecture integration.

TSS inventories NORC-owned devices, which are assigned to named employees and updated in the asset tracking inventory, housed in the BMC Footprints help desk system. Each device is identified by both its personal identification number and a phone number (in the case of smart phones and blackberries).

TSS requires the use of passwords to unlock all NORC-owned smartphones. A second, distinct password is required to unlock the Good Mobile Messaging application.

Additionally, all NORC Windows 7 laptops are configured with WinMagic's SecureDoc Disk Encryption FIPS 140-1 level 2, AES Cert #1 and fully encrypt the hard drive. All NORC laptops are configured with Juniper SSL VPN connection software to allow connection remotely to the NORC network. Without this Juniper SSL VPN software and configuration, all NORC laptops and mobile devices would not be able to connect. Support staff also utilizes Citrix connectivity.

Blackberry Devices, uses cryptographic kernel v3.8.4.47: All email sent to these devices comes from the Exchange server which scans all messages for Viruses. Any e-mail going to these devices has already been scanned and cleared.

The GOOD Mobile application restricts access to NORC email and contact information by providing a quarantined space within the phone to manage all NORC related email and contact information. This quarantined portion of the device is encrypted and password protected,

Domain connected laptops and workstations are configured to update their Viruscan DATs daily and SDATs per administrator release, as well as when logging on (via the logon script). All patches are installed using WSUS and are configured to be scanned for missing patches every 5 days. Additionally, all non-essential services have been disabled using the USCB as a model template. Remote clients are checked for compliance with NORC security policy and controls at each connection initiation.

Personally-owned removable media is explicitly forbidden unless specifically allowed or approved.

NORC has strict guidelines/controls for issuing portable and mobile devices in its environment. The entire life cycle of the device is managed including: requisition, deployment/configuration, system usage, and device recovery. Without the Juniper SSL VPN software and configuration, all NORC laptops and mobile devices would not be able to connect.

4.1.15 AC-20 Use of External Information Systems, including Enhancements AC-20(1) (2)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems as specified in our policies, procedures, contracts, Data Use Agreements (DUA) and rules of behavior. Personally owned information systems are limited to email access and administrative systems are not used to conduct business operations. This is enforced throughout the requirement of network authentication and by the need for a client-side certificate for VPN access. Both of these methods are monitored continuously.

Personally-owned removable media is explicitly forbidden unless explicitly authorized by NORC TSS or ISO and the departmental manager. Only NORC approved removable media can be used.

4.1.16 AC-21 Information Sharing

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC only shares confidential information with business partners who are contractually bound to meet or exceed NORC’s information security and privacy standards and practices. Most typically, business partners and NORC are bound by the terms and conditions defined in a mutually executed Data Use Agreement.

NORC shares confidential information with business partners, on a need-only basis via SFTP. NORC administers access privileges to its SFTP site in accordance with the principle of least privilege. Access requests follow the automated and manual protocols defined in AC-2, “Account Management,” and AC-3, “Access Enforcement.” Activity is monitored at the user level.

4.1.17 AC-22 Publicly Accessible Content

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC designates specific individuals who are authorized to post information onto NORC external websites that are publicly accessible. These designated individuals are restricted

by group permissions on the systems. Individuals must receive supervisor permission before being granted authorization.

NORC trains the authorized individuals to ensure that publicly accessible information does not contain nonpublic information. All staff who posts publically accessible information must complete NORC Security Awareness Training and verify they have read the IT-13 Publicly Accessible Content SOP. This training sufficiently includes information on Personally Identifiable Information (PII) that distinguishes the difference between what data can and cannot be published on publicly accessible websites. NORC maintains a Learning Management System (LMS) training system to track and verify staff has completed the training.

Post-publication reviews are carried out bi-weekly to provide additional assurance that content already posted to NORC websites is not nonpublic in nature.

NORC Information Security Officer(s) conduct a quarterly review of all public NORC web sites for the presence of PII / PHI. If public content is discovered it is removed and may be investigated as a security incident in accordance with NORC Incident Response Plan.

4.2 Audit and Accountability (AU) Controls

4.2.1 AU-1 Audit and Accountability Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Audit and Accountability Policy” which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Audit and Accountability.

The NORC Security Policy Auditing and Accountability Procedures contains documented procedures to facilitate the implementation of the Auditing and Accountability policy and associated Auditing and Accountability controls.

Continuous Monitoring – NORC reviews organization-wide policies and procedures annually, which NORC defines as within 365 days. If any changes are made, NORC policy and procedures are adjusted accordingly

4.2.2 AU-2 Audit Events, including Enhancement AU-2(3)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC servers log the required auditable events on a regular basis and audits the following weekly: account creation, modification, disabling, and deletion as well as administrative permissions executed on user accounts (i.e., inclusion in access groups, reset of password, account lockout override), administrative permissions executed on a system resources (i.e., addition of users or groups to access lists, creation of share points, creation of new access groups, change of access group permissions), failed login attempts and account lockout, use of 'administrator' or equivalent accounts, activity log roll-over, deletion, or editing. In addition, start up and shut down, user log-on and log-off (successful and unsuccessful), configuration changes, and application alerts and error messages are logged and reviewed weekly.

NORC coordinates its security auditing functions with other NORC entities requiring audit-related information in order to enhance mutual support and to help guide the selection of auditable events. The NORC Server Team coordinates with the NORC Network and Database Teams to verify that their respective applications and databases meet the defined auditable event capabilities.

All logs are to be sent to the centralized eIQ SecureVue Security Information and Event Management System (SIEM).

NORC defines, based on current threat information and ongoing assessment of risk, a subset of auditable events in addition to those in regular audit events (see 'Log Collection' events listed above) that are to be audited within the information system and the situation for auditing for each identified event.

NORC employs an automated eIQ SecureVue Security Information and Event Management System (SIEM), to review and analyze information system audit records in near real-time. NORC adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk.

4.2.3 AU-3 Content of Audit Records, including Enhancement AU-3(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC information systems must produce audit records that contain the following types of information:

- What type of event occurred
- When (date and time) the event occurred
- Where the event occurred
- The source of the event
- The outcome (success or failure) of the event, and
- The identity of any user/subject associated with the event

4.2.4 AU-4 Audit Storage Capacity

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded. Group policy objects required by each project configure event log settings accordingly. Additionally functionality for audit log maintenance is provided by the recommended Event Log Checker application.

The minimum standards on audit storage capacity are as follows:

- Three times the storage size of the current daily log file should be free for daily audit archival.
- Ten times the storage size of the current weekly log file should be free for weekly audit archival.

NORC ensures that in the event of audit failure or if audit log capacity is reached, that system administrators are notified. NORC also has an automated system to monitor audit logs.

4.2.5 AU-5 Response to Audit Processing Failures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC ensures that in the event of audit failure or if audit log capacity is reached, that system administrators are notified. eIQ SecureVue Event Management System will notify system administrators and overwrite oldest audit records.

Based on the audit failure, specific actions are taken:

- If Windows audit storage exceeded, the information system will overwrite the oldest audit record on the local system.
- If Storage capacity of local file system exceeded, system administrators must free up or increase storage for use by auditing.
- If audit capturing mechanism failure, system administrators must perform a controlled restart of the auditing mechanism.
- If system hardware/software error system administrators must immediately begin working to remediate the error and restore auditing capability

4.2.6 AU-6 Audit Review, Analysis and Reporting, including Enhancements AU-6(1) (3)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC employs eIQ SecureVue Security Information and Event Management (SIEM) system to continuously monitor and analyze information system audit records in near real-time. SecureVue polls events from server systems every 5 minutes and receives syslog messages from network devices as they occur.

The NORC ISO Network Engineering Team continuously monitors Firewall and IDP traffic for inappropriate or unusual activity. Firewalls and alerts have been configured to send text and/or email alerts to Network Engineers when inappropriate or unusual traffic is detected.

When inappropriate or unusual activity is detected, email alerts are generated and sent to the appropriate ISO team members and Team Leads, as well as the ISO Director.

The NORC Security Team monitors file server access, using Varonis DatAdvantage, upon request by Information Owners to track user access to secure documentation. Activity reports of specific secure project folder are typically shared with Information owners. If an Information Owner determines a user should no longer have access to certain project data, for any reason, ISO will facilitate the access revocation request(s).

NORC utilizes eIQ Secure Vue Security Information and Event Manager (SIEM) to capture, retain and correlate logs to facilitate expedient analysis, investigation and reporting. The ISO Server Administration Team is responsible for the configuration and use of the SIEM to support ongoing information systems availability and early warning of potential threats. Through the use of dashboards and reports, Secure View displays event data by a wide variety of user configurable options.

Once the events are received by the Event Log Management (ELM) system, they are immediately processed and searched for pre-defined log events indicating inappropriate or unusual activity. When inappropriate or unusual activity is detected, email alerts are generated and sent to the appropriate ISO team members and Team Leads, as well as the ISO Director.

The NORC ISO Engineering Team utilizes the SecureVue capabilities to provide an over assessment of the environment, which they use to provide the organization with the situational awareness to facilitate risk-based decisions in support of incident response, contingency planning, infrastructure and environmental investment and audit support. NORC adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk.

4.2.7 AU-7 Audit Reduction and Report Generation, including Enhancement AU-7(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC uses the eIQ SecureVue LMS SIEM software which has reporting capability. Standard and custom reports have been built to review event criteria. Unaltered server logs are retained in eIQ SecureVue for one year.

4.2.8 AU-8 Time Stamps, including Enhancement AU-8(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC information systems use internal system clocks to generate time stamps for audit records. All

NORC information system components use the local time of CST (UTC -0600) or CDT (UTC -0500) during daylight savings time.

NORC uses the Network Time Protocol (NTP) to synchronize the NORC routers with an (external) authoritative time servers every 15 minutes. All devices on the network maintaining time and date information must obtain their time and date from the NORC Network Time Protocol (NTP).

NORC network routers synchronize with external, authoritative time source every fifteen (15) minutes with NIST authoritative time servers at the utcbist.colorado.edu, nist.netservicesgroup.com, time-nw.nist.gov, time-c.nist.gov, and www.nist.gov. NORC Active Directory (AD) Domain Controllers synchronize with those routers to obtain the correct time and effectively become NORC's internal, authoritative time source which all servers and workstations throughout NORC synchronize with to maintain consistent time.

NORC servers and workstations all synchronize with the internal time source every 15 minutes to ensure all systems are on the same internal system clock.

4.2.9 AU-9 Protection of Audit Information, including Enhancement AU-9(4)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The information system protects audit information and audit tools from unauthorized access, modification, and deletion through access controls based on NORC policy. Only SA's have access to the audit logs.

Access to audit records and audit tools on a specific information system component is restricted to system administrators of that component and the eIQ administrator for any logs aggregated within eIQ SecureVue Event Monitoring System (EMS) from such assets. Audit records are backed up weekly to a physically different system than the one being audited.

4.2.10 AU-11 Audit Record Retention

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC retains audit records on its audit logging facilities for adequate times as defined in the records retention policies.to support after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Logs on individual systems are kept for the maximum amount of time that the audit storage capacity of that individual system will allow and these are generally configured to accommodate at least a year of log files online at which point they are then written to digital media for offsite storage for a duration of seven years. The storage capacity of information system components are listed in NORC (AU-4) SOP IT-139, Audit Storage Capacity. NORC may retain audit records for a greater length of time if they are determined to be needed for administrative, legal, audit, or other operational purposes.

4.2.11 AU-12 Audit Generation

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC information systems provide audit record generation capability for the list of auditable events defined in AU-2 at the system device level. The following information system components provide native audit record generation:

- Windows Servers
- Windows Server Components
- Networking Equipment (i.e. Cisco routers and switches)
- Database Applications

NORC information systems only allow designated organizational personnel to select which auditable events are to be audited by specific components of the system.

NORC information systems must generate audit records for the list of audited events defined in NORC (AU-2) SOP IT-38, Event Monitoring, with the content as defined in NORC (AU-3) SOP IT-138, Audit Record Content. This is enforced through the NORC system baseline as defined in CM-2.

4.3 Identification and Authentication (IA) Controls

4.3.1 IA-1 Identification and Authentication Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled “Identification and Authentication Policy” which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to Identification and Authentication. The policy, and associated procedures are disseminated to NORC IT Management, ISO System Engineers, IT Security personnel and TSS personnel.

The NORC Security Identification and Authentication Procedures contains documented procedures to facilitate the implementation of the Identification and Authentication policy and associated Identification and Authentication controls.

Continuous Monitoring – NORC reviews organization-wide policies and procedures within 365 days. If any changes are made, NORC policy and procedures are adjusted accordingly.

4.3.2 IA-2 Identification and Authentication (Organizational Users), including Enhancements IA-2(1) (2) (3) (8) (11) (12)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Each NORC employee and/or project system users must have and use a unique logon name and password. OS logon names are not shared, and users are not allowed to log on under a group account.

NORC Multifactor Summary:
Factor 1: Access point verifies NORC generated security tokens are present on endpoint
Factor 2: Username/password
Factor 3: Digital Certificate

NORC has implemented a 2 factor authentication solution utilizing a cryptographic certificate installed on laptops, which is assigned to both the user and the device. The Juniper VPN controller looks for the presence of the certificate before establishing a link with the NORC domain controller, which prompts the user to enter his/her network password.

Access authentication to internal NORC systems is performed through the use of Microsoft Active Directory logins and Active Directory group membership. NORC utilizes multi-factor authentication for remote access to the information system and conforms to NIST SP 800-53 Revision 4by utilizing “soft” cryptographic digital certificates, in addition to the account identifier and password.

NORC information systems use mechanisms such as TLS version 1.2 or greater for network access to privileged accounts. TLS 1.2 utilizes SHA-256 hashing function, which prevents the replay of password input. This is usually a time-stamp or time varied random number.

Remote access to internal NORC systems is accomplished through the use of moderate multifactor authentication mechanisms. NORC uses a Juniper VPN to provide remote network access, which has been configured to allow remote access to devices that are configured with a NORC-provisioned cryptographic certificate assigned to both the device and the named user.

If the certificate has been successfully validated by the Juniper VPN device, the Juniper device will trigger the NORC Active Directory to authenticate the user. Active Directory requires the user to input his/her NORC network password (something you know). The implementation of network authentication as a step managed outside of the Juniper VPN device, minimizes the risk of compromising the authentication credentials, if they were to be stored directly on the VPN device itself. Active Directory authentication utilizes the Kerberos protocol, which employs SHA-256 hashing algorithms.

Since NORC in not a federal agency, NORC is also not able accept and electronically verify Personal Identity Verification (PIV) credentials from federal agencies.

No CDC users will be accessing the AMSM system; only survey participants.

4.3.3 IA-3 Device Identification and Authentication

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Only ISO administrators can connect devices to the system. A device must be added to the Active Directory group in order to be a part of the NORC Domain. The device must be added to the domain by the Domain Administrator.

4.3.4 IA-4 Identifier Management

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Identification credentials for new NORC employees are vetted through Human Resources and verification is achieved via background checks and E-Verify. HR notifies the Supervisor of the prospective or new employee of the verification results. If the results of identification and background checks are favorable, and the employee is approved for hire, then the Supervisor may request NORC system accesses for the new employee as appropriate, to include an associated identifier for the employee. All requests to add user accounts to the NORC environment or NORC systems must come from the user’s supervisor or system owner.

User identifiers are selected that uniquely identify the new user. A specific convention is in place to establish the format of the identifier.

Assignment of the new user’s, user identifier to appropriate work Groups and devices is achieved using Microsoft Active Directory.   Only users of the NORC IT, Infrastructure, Security and Operations Group, to include TSS, may add or remove users from NORC computing and network environments.

Reuse of identifiers on NORC IT systems is explicitly forbidden.

ISO disables user accounts after a period of inactivity of no more than 60 days or upon receipt of the user termination report – whichever comes first.

4.3.5 IA-5 Authenticator Management, including Enhancements IA-5(1) (2) (3) (11)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:

NORC verifies the identity of the new employee candidate and/or device receiving the authenticator. Once individuals are vetted through Human Resources via a background check, E-Verify or other type of verification medium, the hiring approval for the employee candidate is sent to their prospective Department Head.

Specific rules are in place to format initial authenticators.

Authenticators must meet NORC’s established minimum password requirements. NORC uses CIS Standards:
Account Policy:

1. Minimum Password Age: 1 day
2. Maximum Password Age: 90 days (60 days for privileged accounts)
3. Minimum Password Length: 8 characters (15 characters for privileged accounts)
4. Password Complexity: Enabled. Must contain 3 out of 5 of the following items:
    a. Upper Case
    b. Lower Case
    c. Number (0-9)
    d. Special character
    e. Not contain same 3 consecutive characters of the userid.
5. Password History: 24 passwords remembered
6. Passwords are encrypted in storage
7. Temporary passwords must be changed upon initial login

NORC has administrative procedures in place for forgotten or compromised authenticators. In the case that authenticators, particularly passwords, are forgotten or compromised, employees must call Technology Support Services (TSS). All user accounts are locked for 15 minutes after three failed attempts to login to that account. Forgotten passwords are currently changed by the TSS group following a submission of a trouble ticket from the user's manager or a phone call to the TSS group.

When new equipment is installed authenticators are always changed from the vendor default authenticators to the authenticators driven by best practices and NORC policies.

NORC encrypts passwords in transmission using Kerberos encryption provided with Active Directory (i.e. during log-on etc.). As users type passwords, the characters are hashed to minimize the risk of a replay attack.

Users shall immediately notify their supervisors, IT Security Compliance and the NORC help desk in order to change their passwords if they suspect it has been compromised. Passwords must not be stored in clear text or in any easily reversible form in batch files, automatic login scripts, software macros, terminal function keys, or in any location where an unauthorized person might discover them. Passwords must not be hard-coded into software.

Shared user accounts (e.g., generic, administrator, guest, temporary) are not permitted.   Access to built-in identifiers is restricted to ISO Team members only. Passwords must be changed within 30 days of ISO Team personnel changes.

Certificates are generated by a trusted root CA: Symantec TrustCenter. TrustCenter maintains a valid certificate chain between the certificate and the CA.

Private keys are not exportable and are protected by a PIN, known only to the certificate owner

The process for obtaining a certificate is as follows:

1. User requests approval from the department head
2. Once approval is obtained, the user opens a help desk ticket requesting a certificate
3. Upon verifying the approval, a certificate is generated at the CA's operations portal.
4. The CA generates the certificate
5. The CA sends the user, via email, the private key PIN
6. The CA sends the user a password for accessing the operational portal and a link to their certificate.

NORC verifies the identity of the new employee candidate and/or device receiving the authenticator. Once individuals are vetted through Human Resources via a background check, E-Verify or other type of verification medium, the hiring approval for the employee candidate is sent to their prospective Department Head.

No CDC users will be accessing the AMSM system; only survey participants.

4.3.6 IA-6 Authenticator Feedback

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The Operating System (OS) and SQL database provides feedback to the user during an attempted authentication without compromising the authentication method. For example, asterisks are displayed when the user types in a password and a user is notified if the Caps lock is on login reveals that the feedback for authentication is obscured in order to protect the information from exploitation for operating system and applications.

4.3.7 IA-7 Cryptographic Module Authentication

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC uses WinMagic's SecureDoc Disk Encryption FIPS 140-2 level 2 for all field laptops. FIPS 140-2 level 2 is accompanied with the crypto module validation AES (256-bit) encryption algorithm with certificate number 1

- Juniper FIPS 140-2 (1026)
- RIM Blackberry (827), Using cryptographic kernel v3.8.4.47
- WinMagic (209)
- eIQ Security Information and Event Management (SIEM)
- WinMagic's SecureDoc Disk Encryption is Identity-Based and provides Laptop full-disk encryption.
- Windows OS cryptographic libraries is identity-Based and provides Authentication, local encryption, TLS.
- Juniper VPN Gateway is Identity-Based and provides Remote VPN access.

4.3.8 IA-8 Identification and Authentication (Non-Organizational Users), including Enhancements IA-8(1) (2) (3) (4)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC is using social media to recruit respondents, so potentially eligible respondents will see an ad on Facebook, Instagram, Snapchat or Kik. If they click the ad, they'll be taken to the AMSM website, and will go through the process of consent -> screener -> full survey. If they aren't eligible, they will not be able to continue on to the survey, but the survey webpage isn't separate from the screener webpage. That is, it's all one system. Anyone who meets the criteria may be shown an ad for the survey, and thus be able to access the weblink.

No CDC users will be accessing the AMSM system; only survey participants.

4.4 System and Communications Protection (SC) Controls

4.4.1 SC-1 System and Communications Protection Policy and Procedures

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC has developed and maintains a policy entitled "System and Communication Protection Policy" which defines the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to System and Communication Protection. The policy is posted to the NORC LANADM shared drive for review and guidance by IT Management, ISO and TSS personnel.

NORC has developed and maintains a procedural document entitled "System and Communication Protection Procedures" which define the purpose, scope, roles, responsibilities, management, commitment, coordination, and compliance controls relating to System and Communication Protection.

Continuous Monitoring – NORC reviews organization-wide policies and procedures within 365 days. . If any changes are made, NORC policy and procedures are adjusted accordingly.

4.4.2 SC-2 Application Partitioning

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
All NORC information systems are partitioned based on system function and least privilege access. System functions that are of different types, database vs. application for example, are placed on different servers. Access to any system component is restricted only those who require the service to perform the functions of their jobs.

The NORC networking and computing infrastructure has been created to support the physical partitioning of applications. As a rule all production databases run on servers that only support production database activity. Applications run only on servers designated for the specific project and application activity. Application users are never granted direct access (e.g RDP, modify share) to any application. In addition to separate physical platforms, each platform is maintained and managed by a different infrastructure administrative group.

The majority of NORC custom software is built using the 1) Java based NORCSuite application framework, 2) the ASP.NET based Liberty application framework or 3) the python/django Data Science framework.

All of these frameworks enable the construction of applications that use the MVC (Model-View-Controller) software architecture standard. In this standard the Model represents the business or database code, the View represents the page design code, and the Controller represents the navigational code.

4.4.3 SC-4 Application Partitioning

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
This capability is an inherent function of the operating systems employed by NORC. Shares are limited and monitored and are assigned by specific projects and have a limited lifespan in line with the data collection schedule. In addition, the SFTP is secured by directory permissions to prevent inadvertent file transfer.

4.4.4 SC-5 Denial of Service Protection

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC information system protects against or limits the effects of the following types of denial of service attacks: ICMP, UDP and SYN floods, SYN cookie attached, SYN Random Early Drops, Teardrops, Low-rate, Peer-to-Peer, Asymmetry of resource utilization, Application-level floods, and Unintentional DOS attacks, by employing stateful packet-filtering firewalls, which send alerts to NORC’s SIEM to provide alerts and ongoing monitoring by NORC Network Engineers, who can respond and make adjustments to firewalls and IDP devices to prevent these attacks and resume normal operations.

4.4.5 SC-7 Boundary Protection, including Enhancements SC-7(3) (4) (5) (7)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:

The NORC network is designed such that boundaries are protected via appropriate interfaces and employs tools that monitor communications at these points. In addition, NORC restricts confidential data from being stored on a public network.

NORC physically allocates publicly accessible information system components to separate sub-networks with separate, physical network interfaces.

Specific managed devices provide boundary protection and are established with a default deny-all architecture, allowing only specifically-allowed devices and services to cross.

NORC Engineering Network Team does review outbound traffic flow requirements for exceptions, (both additions and revocations), against business and operational needs on a quarterly basis.

NORC maintains managed interfaces' for each of its external telecommunication services. NORC has a traffic flow policy for each of its managed interfaces. NORC managed interfaces', denies network traffic by default; and allows network traffic by exception.

NORC restricts confidential data from being stored on a public network.

NORC ISO Network Engineers document proposed traffic flow exceptions in Security Impact Analyses, which are reviewed by the NORC IT Change Control Board as part of the Change and Configuration Management process. This documentation includes the business justification and/or explanation for the requested exception. These documents are retained secure IT file shares as ongoing documentation of these exceptions.

NORC Engineering Network Team executes a quarterly audit of all traffic flows, and open TCP ports, which includes reviews of inbound and outbound traffic flow requirements for exceptions, (both additions and revocations), against business and operational needs on a quarterly basis. Follow-up action includes configuration adjustments to close TCP ports and traffic routes that are no longer in use or necessary to enable business operations.

Boundaries are established with a default deny-all architecture, allowing only specifically-allowed devices and services to cross.

4.4.6 SC-8 Transmission Confidentiality and Integrity, including Enhancement SC-8(1)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
The NORC infrastructure is a switched network, which enhances the confidentiality and integrity of transmitted information. NORC uses fiber optic cable to connect infrastructure equipment between floors. All network and telecommunication equipment is housed in locked facilities.

Based on the guidelines in NIST SP 800-52, NORC uses TLS protocols to initiate and protect VPN tunnels for employee remote access. TLS protocols are also employed by external Web servers where sensitive data may be transmitted. All cipher suites and key exchange mechanisms met FIPS 140-2 guidelines.

NORC uses the following methods to provide transmission confidentiality and integrity:

- Checksums defined by the TCP and UDP networking protocols.
- Checksums provided by the IPv4 header.

- Cryptographic mechanisms as defined in Section 4.1 above and 4.3 below.
- Enforcement of SMB signing.
- Switches and transmission lines are physically secured
- Operating system protection mechanisms against common spoofing and man-in-the-middle attacks.

4.4.7 SC-10 Network Disconnect

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Connection termination at the end of a session is an inherent function of the operating systems employed by NORC. Users must re-authenticate to the System (e.g. unlock password-protected screen savers) if session is idle for more than 15 minutes.

4.4.8 SC-12 Cryptographic Key Establishment and Management

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC ISO Engineering Team is responsible for the establishment and management of cryptographic keys, which must contain the following characteristics:

- The private key component of the key pair must be kept confidential to ensure its proper use.
- Keys must meet requirements of FIPS 140-2 compliant algorithms and hashes.
- Proper lifecycle management of keys.
- Proper key backup and recovery procedures.

4.4.9 SC-13 Cryptographic Protection

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
Encryption of Data at Rest - NORC protects data in its custodial control via encryption at rest on its drive arrays, utilizing AES 256 bit encryption. Keys are administered by a key generator and stored in a lockbox on the arrays. A Key Manager monitors the status changes of encryption keys, which are reset each time the array reboots. Data encryption keys are encrypted themselves prior to movement within the array.

Backups - All NORC tape backups are encrypted using a HP MSC 6480 81 library hardware encryption method. The LTO-6 library drive provides native encryption functionality using AES 256 bit encryption.

Wireless LAN - Guests must obtain an SSID password from a sponsor. Credentials are verified by the NORC AD domain controller. NORC has implemented WPA2, Pre-shared Key (PSK) network authentication with AES encryption for guest SSID access.

End User Devices - all NORC Windows 7 laptops are configured with WinMagic's SecureDoc Disk Encryption FIPS 140-1 level 2, AES Cert #1 and fully encrypt the hard drive. All NORC laptops are configured with Juniper SSL VPN connection software to allow connection remotely to the NORC network. Without this Juniper SSL VPN software and configuration, all NORC laptops and mobile devices would not be able to connect. Support staff also utilizes Citrix connectivity.

Passwords - NORC encrypts passwords in transmission using Kerberos encryption provided with Active Directory (i.e. during log-on etc.).

4.4.10 SC-15 Collaborative Computing Devices

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
N/A - Collaborative computing is not allowed on the AMSM system.

4.4.11 SC-17 Public Key Infrastructure Certificates

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC ISO Engineering acquires, deploys and Manages PKI certificates from Network Solutions and DigiCert to protect various service components in the NORC information system. In addition, ISO Engineering manages an internal PKI certificate server, which issues certificates signed and validated by SecureAuth. Over 60 certificates cover a variety of NORC web-based services that may contain sensitive data.

Two factor authentication is currently implemented for remote telework access into the NORC network. Individual certificates are issued from Symantec Corp. A new user is issued a certificate from the Symantec portal. The user receives two emails that are used for the user to download their individual certificate. The user must import the certificate into their local computer’s profile. Upon login of the Juniper SSL VPN, before the user’s credentials are sent for authentication, the Juniper SSL VPN verifies that the user has a local certificate installed. Without a certificate, the login fails with a “Missing certificate” error message. Once the certificate is validated, the user’s credentials are sent to the authentication server to be authenticated.

4.4.12 SC-18 Mobile Code

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC enforces a locked-down workstation configuration that prevents the installation of unauthorized mobile code.

NORC must keep mobile code related software and patches up to date to limit flaws and known vulnerabilities. NORC uses network vulnerability scanning software to detect any vulnerable mobile code technology deployed on the NORC infrastructure or versions of Mobile Code not on an approved configuration baseline. Further detail is provided in NORC SOP IT-20 Mobile Code Implementation.

NORC monitors mobile code software deployed in the system to ensure software does not contain critical flaws that may contain malicious code or contain security vulnerabilities. NORC also conducts vulnerably scanning on the network to identify possible flaws in mobile code technologies.

4.4.13 SC-19 Voice Over Internet Protocol

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
VOIP is employed only for internal phone communications. Communications are monitored for misuse via reporting and billing information. NORC firewalls also restrict the ability to make long distance calls without inputting a specified code that is traceable. NORC authorizes, monitors and controls the use of VoIP within the information system.

4.4.14 SC-20 Secure Name / Address Resolution Service (Authoritative Source)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
All active directory integrated DNS servers are redundant. NORC currently has six redundant DNS servers. Only computers in the domain access Active Directory DNS. AD integrated Domain Name Services (DNS) enables ever domain controller within the domain to act authoritatively.

All Domain Controllers are authoritative. Redundant sites are separated both logically and geographically to ensure fault-tolerance. Internally, NORC uses 10 DNS servers geographically disbursed throughout the company.

4.4.15 SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
All of NORC DNS servers are configured using active directory integrated Dynamic DNS (DDNS) – Only authenticated systems are able to request lookups subsequently only authenticated systems are able to add DNS entries to NORC DDNS Zones. Resolution of DNS lookups are handled by DDNS using only secure dynamic updates from authoritative sources. NORC DNS Servers cache DDNS requests for a period of 4 hour and then are discarded by timeout. All Clients are unable to request unsecure\ unauthoritative DNS lookups from any NS, DNS, or DDNS servers that have not been explicitly defined as a member or the Active Directory Integrated DNS infrastructure.

4.4.16 SC-22 Architecture and Provisioning for Name / Address Resolution Service

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC uses Microsoft Active Directory integrated DNS services. All domain controllers are configured as DNS servers. These servers provide name resolution services for clients attached to NORC's internal LANs only. DNS updates are encrypted and only allowed to NORC's integrated zones for transfer. (Active Directory Integrated DNS zone transfers).
NORC employs a Split DNS schema. External name resolution, provide by a third-parting hosting service, is separate from internal name resolution. Four name servers, on two different IP subnets, are configured for external queries.

4.4.17 SC-23 Session Authenticity

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
All DNS information is encrypted and uses signed certificates for replication between all of the domain controllers in the domain. NORC uses TLS protocols to initiate and protect VPN tunnels for employee remote access. TLS protocols are also employed by external Web servers where sensitive

data may be transmitted. All cipher suites and key exchange mechanisms met FIPS 140-2 guidelines.

4.4.18 SC-28 Protection of Information at Rest

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC keeps the confidentiality and integrity of the data intact by logical and physical controls. Limited access to the data is granted through Active Directory groups following the least privilege model. Only the users that need access to the data for their job function are granted access.

NORC utilizes AES-256 encryption within its EMC array environment to protect the confidentiality and integrity of information-at-rest as its default policy. In addition, NORC ISO Engineering maintains a Varonis DatAdvantage system, which contains functionality to scan file servers for certain types of information (PII no longer required by current project work) to facilitate activities around ongoing monitoring of data that should be destroyed in accordance with the controls described in NORC SOP, IT-104 (MP-6) Media Sanitization.

NORC also encrypts information-at-rest on databases as required by specific client projects, and/or as directed by the client. This requirement generally applies to systems that house sensitive data, such as PII and/or PHI data, but is not implemented by default.

All encryption technologies employed must be FIPS 140-2 compliant.

4.4.19 SC-39 Process Isolation

Control Implementation Status: In Place

Control Effectiveness: Fully Satisfied

Control Type: System

Common Control: None.

Compliance Description:
NORC IT utilizes a combination of hardware and software controls in its servers, applications and endpoints to maintain separate execution domains for executing processes.
System Administrators maintain development, testing and production environments to ensure that production data is unaltered during the application development process. Servers are configured to utilize the processing isolation components of the operating systems in use: Windows and Linux. Further, IIS (web services) and MS SQL (database services) provide additional process isolation protection.
Segregation of Duties: Application Developers are restricted from executing any changes in production environments; System Administrators promote code to production upon completion of testing and authorization by Senior Managers, who review functionality and test results.
Application developers program in object-oriented languages, in which they build objects with high cohesion and low coupling, utilizing sandboxes and virtual machines to ensure that code is executed within its own execution domains.
Desktop machines and servers are routinely patched for security and anti-virus updates to mitigate the risk of execution domain compromises as a result of a security flaw or attack.