1. General Information

1.1. CIPSEA Protection Plan for NORC AmeriSpeak

1.2. NORC POC :

Name:	J. Michael Dennis
Address:	55 E. Monroe, 30th Floor, Chicago Illinois 60603 Dennis-Michael@norc.org
Phone:	650-537-7950

1.3. Government POC:

Name:	Krystal Tomlin
Title:	Resource Management Specialist
Office Address:	3311 Toledo Road, Hyattsville, MD 20782
Work Phone:	301-458-4189
e-Mail Address:	Ktomlin@cdc.gov

1.4. General Description/Purpose: What is the function/purpose of the NORC AmeriSpeak Service? **[Provide a short, high-level description of the function/purpose of the service.]**

NORC'S AmeriSpeak Panel provides a scientific sample of pre-recruited U.S. households that have agreed to participate in public opinion and other surveys. Since its founding by NORC at the University of Chicago in 2015, AmeriSpeak has conducted more than 250 surveys; been cited by dozens of media outlets; and has become the primary survey partner of the nation's preeminent news service, *The Associated Press.* AmeriSpeak randomly identifies Americans, including the country's hardest-to-reach populations, and recruits them to provide their opinions and insights on a wide range of topics critical to our clients. The outcome is a truly representative picture of America and, thus, more accurate research results.

General Description of Information: The target information that NORC is compiling via its AmeriSpeak offering is not US Government information. However, as it will be correlated with NCHS information once delivered, NCHS is requiring NORC compliance with the Confidential Information Protection and Statistical Efficiency Act Statistical Efficiency Act (44 U.S.C. 3561-3583) as detailed within the Designated Agent Agreement (DAA) between NCHS and NORC.

Authorized User, also referred to as Designated Agent, is defined as a person who has completed NCHS confidentiality training (https://www.cdc.gov/nchs/training/confidentiality/training/), submitted a certificate of completion for the training, and signed the NCHS affidavit of nondisclosure.

CIPSEA Information refers to the sampling frame information and data collected under this project.

2. NORC ENVIRONMENT

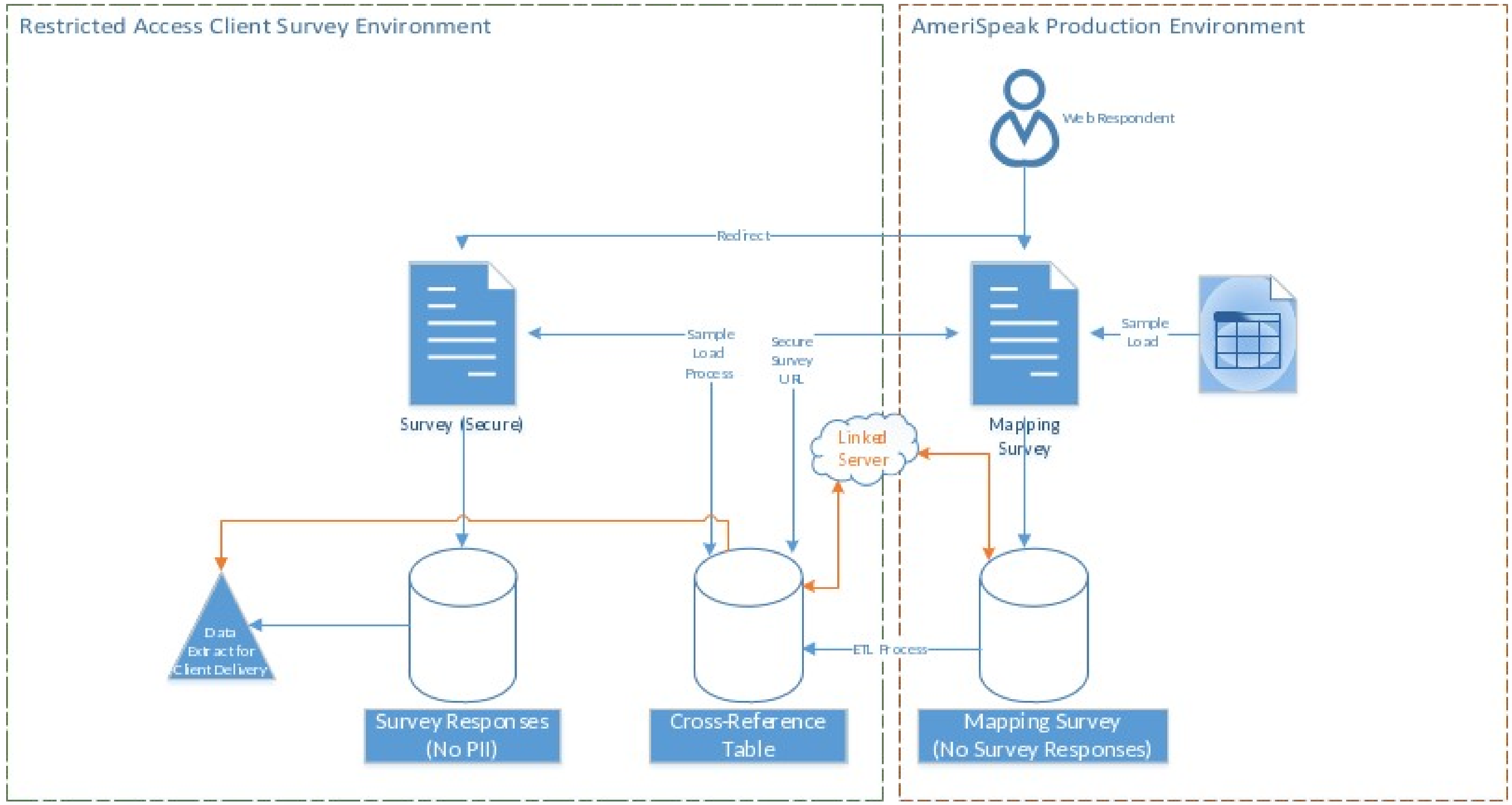
[Provide a narrative consistent with the graphic that clearly lists and describes each component.]

The target information that NORC is compiling via its AmeriSpeak offering is not US Government information. However, as it will be correlated with NCHS information once delivered, NCHS is requiring NORC compliance with Confidential Information Protection and Statistical Efficiency Act Statistical Efficiency Act (44 U.S.C. 3561-3583) as detailed within the Designated Agent Agreement (DAA) between NCHS and NORC.

Authorized User, also referred to as Designated Agent, is defined as a person who has completed NCHS confidentiality training (https://www.cdc.gov/nchs/training/confidentiality/training/), submitted a certificate of completion for the training, and signed the NCHS affidavit of nondisclosure.

CIPSEA Information refers to the sampling frame information and data collected under this project.

Secure Survey – Solution Design


Restricted Access Client Survey Environment
AmeriSpeak Production Environment
Web Respondent
Redirect
Survey (Secure)
Sample Load Process
Secure Survey URL
Mapping Survey
Sample Load
Linked Server
Data Extract for Client Delivery
ETL Process
Survey Responses (No PII)
Cross-Reference Table
Mapping Survey (No Survey Responses)

Notations:

+ Separate secure environment will house client survey and associated survey response data.
+ Cross-reference table houses mapping details between environments and is only accessible by secure service account and approved DBA resource.

3. PROTECTIONS

Provide a thorough description of how all of the protections are being implemented or planned to be implemented. The description for each protection contains: 1) the protection number and description; 2) how the protection is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the protection is not applicable to the NORC AmeriSpeak service, provide rationale.

3.1. Logical/Physical Access Control

3.1.1. Limit system access where CIPSEA Information is stored and processed to authorized users (as defined in Section 1.5 of this document), processes acting on behalf of authorized users, and devices (including other systems).

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Permissions are granted on a per project basis. Users must be approved by project directors prior to access being granted to the user.
- Microsoft Active Directory are used to restrict access to all information systems. Authorized users access and processes acting on behalf of the authorized users are validated against Microsoft Active Directory before allowing accessing to any information system data.
- Devices must be joined to the NORC domain to access the system.

3.1.2. Limit system access to the types of transactions and functions that authorized users (as defined in Section 1.5 of this document) are permitted to execute.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Access is limited by job function. Interviewer, supervisors and administrators are given appropriate access to perform their job functions.

3.1.3. Control the flow of CIPSEA Information in accordance with approved authorizations.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All data is kept within the Amerispeak system boundary.

3.1.4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide

rationale.

- Individuals are assigned one permission for one job function. Developers are not given administrator privileges.

3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All users with escalated privileges go through a separate approval process. They are given a separate account to perform their security and privileged function from.

3.1.6. Use non-privileged accounts or roles when accessing nonsecurity functions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All users with escalated privileges go through a separate approval process. They are given a separate account to perform their security and privileged function from.

3.1.7. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Administrative function are limited to the IT departments. Non-privileged users are not granted administrative privileges.

3.1.8. Limit unsuccessful logon attempts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable
Current implementation or planned implementation details. If "Not Applicable," provide rationale.

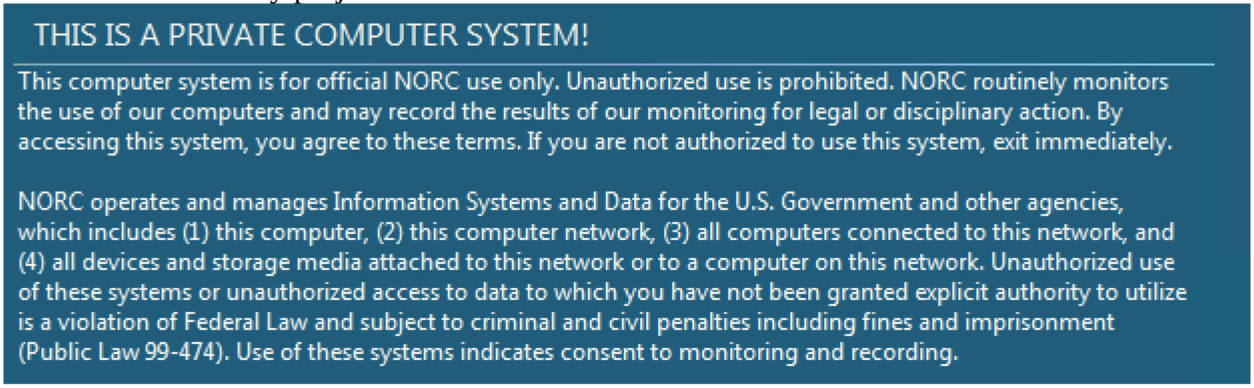
- Unsuccessful logons are limited by Active Directory policy. Accounts are locked after 3 unsuccessful logons.

3.1.9. Provide system use warning banners.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- System warning banners are implemented on all servers and applications.
- This is our actual banner page. This is a shared banner screen for all our systems. It cannot be customized by project.



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.

3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Session lock are implemented by Active Directory policy at 15 minutes.
- User must enter their password to unlock the session. The password is display as dots on the screen.

3.1.11. Terminate (automatically) a user session after a defined condition.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- User sessions are terminate at log off and after a defined inactivity.

3.1.12. Monitor and control remote access sessions.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All remote access sessions are logged by the Juniper VPN concentrator.
- All Juniper logs are collected by SIEM tool for reporting and alerting.

3.1.13. Remote access to CIPSEA protected information (e.g. sampling frame) is not permitted as per the DAA. For all other remote access, NORC employs cryptographic mechanisms to protect the confidentiality of remote access sessions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Juniper VPN concentrator encryption standards meets the FIPS 140-2 standard.

3.1.14. Route remote access via managed access control points.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All remote access is routed through a pair of Juniper VPN concentrators. There is no other remote access allowed into the network.

3.1.15. Authorize remote execution of privileged commands and remote access to security-relevant information.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Users must authenticate into the remote access system with their regular user account. Their privilege account does not have access to login into the VPN remote access system. After they log into the VPN with their regular account with their two factor authentication, they use a separate privilege account to execute privilege commands.

3.1.16. Authorize wireless access prior to allowing such connections. FIPS 140-2 standards are employed to the extent practicable.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The wireless device must be joined to NORC domain and user must have an Active Directory account before the user is allowed to connect to the wireless.
- The wireless network uses the encryption settings according to the FIPS 140-2 standard.

3.1.17. Protect wireless access using authentication and encryption. FIPS 140-2 standards are employed to the extent practicable.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All users must authenticate to access the NORC network over the wireless network.

- The wireless device must be joined to NORC domain and user must have an Active Directory account before the user is allowed to connect to the wireless.
- The wireless network uses the encryption settings according to the FIPS 140-2 standard.

3.1.18. Control connection of mobile devices.

□ Implemented □ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The Amerispeak and CIPSEA protected information cannot be accessed by a mobile device.

3.1.19. Encrypt all information on mobile devices/portable storage/media and mobile computing platforms in accordance with FIPS 140-2 to extent practicable.

□ Implemented □ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The Amerispeak and CIPSEA protected information cannot be accessed by a mobile device.

3.1.20. All information will be processed on NORC enterprise IT assets.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All systems are run on NORC hardware administrated by NORC personnel.

3.1.21. Minimize the use of portable storage devices.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC disables USB drives on all data collection systems. For systems that require their USB drive enabled, they have their portable storage devices automatically encrypted by the full disk encryption WinMagic software installed on the device. The device can only be read by machine with the same WinMagic software.

3.1.22. CIPSEA Information is not posted or processed on publicly accessible systems.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All CIPSEA information is processed on NORC private network which is not accessible from the Internet. The CIPSEA is not posted on any publicly accessible systems.

3.2. Awareness and Training

3.2.1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All NORC employees and contractors must complete annual Security Awareness training.

3.2.2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All NORC employees and contractors must complete annual Security Awareness training.

3.2.3. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.3. Audit and Accountability

3.3.1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- System logs are maintained online for 9 months.

3.3.2. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All access to unstructured data and databases are logged.
- Varonis DatAdvantage tools tracks all access to unstructured data. Idera diagnostics are used to log all activities on SQL databases
- SecureVue SIEM tools collects all server event logs.

3.3.3. Review and update logged events.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Logged events are continuously monitored using a SIEM tool SecureVue. Alerts are sent to appropriate personnel.

3.3.4. Alert in the event of an audit logging process failure.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- SecureVue is set to alert the Engineering team if there are any log failures.

3.3.5. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC uses a combination of alerts and schedule reports to identify unlawful, unauthorized and suspicious activity.

3.3.6. Provide audit record reduction and report generation to support on-demand analysis and reporting.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- SecureVue supports automated alerts and regular scheduled reports.

3.3.7. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- In order to ensure internal systems' clocks are correct and consistent across the enterprise, NORC information systems must synchronize those internal information system clocks with an external, authoritative time source on a defined frequency. NORC uses the Network Time Protocol (NTP) to synchronize the NORC routers with the following (external) NIST authoritative time servers at least every 15 minutes, but will increase the polling frequency if NORC systems fall out of sync.

3.3.8. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- This protection is implemented using access controls based upon NORC policy that are described in NORC (AC-3) SOP IT-02, Access Enforcement and NORC (AC-6) SOP IT-04, Least Privilege.
- Access to audit records and audit tools on a specific information system component is restricted to system administrators of that component.

3.3.9. Limit management of audit logging functionality to a subset of privileged users.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Access to audit records and audit tools on a specific information system component is restricted to system administrators of that component.

3.4. Audit and Accountability

3.4.1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. 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.

3.4.2. Establish and enforce security configuration settings for information technology products employed in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. 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.

3.4.3. Track, review, approve or disapprove, and log changes to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. NORC hardware, firmware, software, and configuration changes must be approved by one of the following:
- • ISO Director
- • IT Functional Director
- o Director of Administrative Systems
- o Director of IT Project Services
- o IT Director, Information Security Officer
- • Network Team Manager
- • Server Team Manager
- • IT Information Security Manager

3.4.4. Analyze the security impact of changes prior to implementation.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The NORC ISO Group analyzes major information system changes to determine potential security impacts prior to change implementation. As part of the configuration change control procedures outlined in IT-94, Security Configuration Settings standard operating procedures (SOP), at the time of initial analysis of a change request, the NORC IT Change Control Group

(IT CCG) determines whether the proposed change will alter the security posture of the Information System.

3.4.5. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system using a variety of methods. Physical access to information system equipment and locations is restricted. Logical access to information system administration software and resources is also restricted. These restrictions allow only authorized personnel to conduct approved changes on NORC information systems.
- NORC policy restricts system administrators from performing changes impacting primary services during core availability hours unless in a defined maintenance window or in emergency circumstances. The core availability hours are established by the NORC Infrastructure, Security, and Operations (ISO) with guidance from NORC management. Changes affecting users must be conducted outside of these availability hours. NORC policy also requires that major changes to the information system follow the change management process as outlined in IT-94 Security Configuration Settings (CM-3) and Change Control Process. This process provides oversight to information system changes.
- NORC restricts authorized physical access to information system resources in a variety of ways. NORC servers and network equipment must be placed in secure locations, specifically within a designated Zayo data center, within NORC's server racks. Network equipment is either maintained in the aforementioned locations or in separate locked cages as needed. Physical access to these locations is restricted to only those personnel requiring access to complete their assigned duties. Further information may be found in NORC's Physical and Environmental Controls SOPs.

3.4.6. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Unneeded functionality, program execution, and network access on Windows assets are disabled using Active Directory (AD) Group Policy. Group Policy objects are configured using industry best practices, NIST guidelines, and Center for Internet Security Baselines. Group Policies are reviewed regularly. NORC systems run local stateful packet filtering firewalls which are configured with a default "deny-all" policy. Ports are only opened on the local firewall if there is an explicit application/business need.

3.4.7. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC system and network administrators are trained in and adhere to the following guiding principles:
    1. NORC must configure systems to provide only essential capabilities as defined by the systems purpose and function.
    2. Unneeded functionality, program execution, and network access on Windows assets are disabled using Active Directory (AD) Group Policy. Group Policy objects are configured using industry best practices, NIST guidelines, and Center for Internet Security Baselines. Group Policies are reviewed regularly. NORC systems run local stateful packet filtering firewalls which are configured with a default "deny-all" policy. Ports are only opened on the local firewall if there is an explicit application/business need.

3.4.8. Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC configures the default firewall and software execution settings for its information systems to deny-all, allow by exception.

3.4.9. Control and monitor user-installed software.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC develops, documents and maintains an inventory of its information systems components that accurately reflects the current information systems' postures and is consistent with the authorization boundary of the system.
- NORC updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

3.5. Identification and Authentication

3.5.1. Identify system users, processes acting on behalf of users, and devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Users are uniquely identified and authenticated for all accesses in which they are approved.

- Each organizational user of the information system is assigned an unique username as a system identifier. The user's unique username will be used system wide to identify the user for all access to the information system.

3.5.2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC identifies and authenticates organizational users at the information system level. Prior to accessing the information system, users must authenticate locally. Once they have authenticated locally, users may then access network resources. Network authentication may re-prompt the user for authentication or authenticate using a process acting on behalf of a user. In addition to identifying and authenticating users at the information system level, identification and authentication mechanisms are employed at the application level, when necessary.

3.5.3. Use multifactor authentication19F for local and network access20Fto privileged accounts and for network access to non-privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC utilizes multi-factor authentication only for remote access to the information system and conforms to NIST SP 800-63 level 3 requirements. All NORC remote users logging onto the network are required to authenticate with two factors, regardless of privilege status.

3.5.4. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All password are obfuscated when they are entered into the application.
- The authentication process is protected by TLS encryption.

3.5.5. Prevent reuse of identifiers for a defined period.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC does not remove accounts from the system for at least 180 days to avoid reuse of the account.

3.5.6. Disable identifiers after a defined period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide

rationale.

- User accounts are automatically disabled after 90 days of inactivity.
- Administrator accounts are automatically disable after 60 days of inactivity.

3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- User passwords must be at least 8 characters, must contain upper and lower case, numbers and at least one special character. Passwords must be changed every 90 days.
- Administrator passwords must be at least 15 character, must contain upper and lower case, numbers and at least one special character. Passwords must be changed every 60 days.

3.5.8. Prohibit password reuse for a specified number of generations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Passwords must not be the same as any of the previous 24 passwords.

3.5.9. Allow temporary password use for system logons with an immediate change to a permanent password.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All accounts are setup with temporary passwords. User must change their password after the first login.

3.5.10. Store and transmit only cryptographically-protected passwords.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- 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.

3.5.11. Obscure feedback of authentication information.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Passwords are not displayed during logon.
- Feedback on failed logons does not identify the problem only the login failed.

3.6. Incident Response

3.6.1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The incident response life cycle is outlined in NIST SP 800-61 and includes four steps:
  - Preparation,
  - Detection and analysis,
  - Containment, eradication and recovery, and
  - Post incident activity.

  These four steps can be thought of as an unending cycle which defines the incident response program. Figure 2-1 shows this cycle as depicted by NIST in SP 800-61.

- Incident response controls must be established and applied to all NORC information systems related to security and privacy matters. Incident response procedures must be performed and documented in the system security plan during the Planning & Requirements Definition Phase and carried out during the Operations & Maintenance Phase of the system development life cycle in accordance with the NORC System Development Life Cycle Manual (SDLCM) to ensure that the most cost effective and appropriate measures are employed. Unless otherwise specified, all NORC information systems are required to comply with the procedures in this section.

3.6.2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC coordinates incident handling activities with contingency planning activities.
- NORC also incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. Sources used for improving upon prior incident response plans are obtained from different sources including, but not limited to, audit monitoring, network monitoring, and user/administrator reports.

3.6.3. Test the organizational incident response capability

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC conducts testing and/or exercises of its incident response capability for its information systems using a combination of IR events specified above. At a minimum, NORC conducts testing and/or exercises of its incident response capability on an annual basis to determine the incident response effectiveness and gaps in the current IR Plan, then documents the results of the IR test and/or exercise.

3.7. Maintenance

3.7.1. Perform maintenance on organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The maintenance procedures must be performed during the Planning & Requirements Definition Phase and periodic maintenance must be performed during the Operations & Maintenance Phase in accordance with the SDLCM.
- NORC schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

3.7.2. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- 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 personnel must 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.

3.7.3. Ensure equipment removed for off-site maintenance is sanitized of any CIPSEA Information.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- 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.

3.7.4. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- 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.

3.7.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Users accessing the system from outside the NORC network must use the NORC provided SSL VPN gateway. The SSL VPN requires multifactor authentication to establish a session.
- All sessions are terminated when a user logs off the SSL VPN.

3.7.6. Supervise the maintenance activities of maintenance personnel without required access authorization.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Any personnel or organization performing maintenance that is not in the above list must be accompanied by an approved maintenance personnel member at all times.

3.8. Media Protection

3.8.1. Protect (i.e., physically control and securely store) system media containing CIPSEA Information, both paper and digital.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC restricts access to digital and non-digital media alike. Only authorized IT Department Staff have access to NORC digital media that contains information form NORC servers. All employees are notified in NORC Policy K7 – Portable Media of what NORC defines as digital, portable and non-portable media. Information system media includes both digital media non-digital media.

3.8.2. Limit access to CIPSEA Information on system media to authorized users (as defined in Section 1.5 of this document).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide

rationale.

- 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.

3.8.3. Sanitize or destroy system media containing CIPSEA Information before disposal or release for reuse.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- 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, computer hard drives, and optical media (CD and DVD). 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. NORC sanitizes data by project as necessary, including comingled database data by running scripts to delete or overwrite records by project ID key, if applicable.

3.8.4. Mark media with necessary CIPSEA Information markings and distribution limitations.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC marks, as applicable and 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.

3.8.5. Control access to media containing CIPSEA Information and maintain accountability for media during transport outside of controlled areas.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- CIPSEA data will remain on NORC disk storage array in the NORC datacenters. CIPSEA data will not be copied to tape and sent our Iron Mountain.

3.8.6. Implement cryptographic mechanisms to protect the confidentiality of CIPSEA Information stored on digital media during transport unless otherwise protected by alternative physical safeguards.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- 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-6 magnetic tape data storage media. CommVault encrypts all backups with AES-256 data encryption, in accordance with FIPS 140-2 guidelines.

3.8.7. Control the use of removable media on system components.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- 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.
- NORC has established strict controls over the use of portable media. When an unidentified portable storage device is inserted into a NORC-owned, encrypted corporate device, WinMagic allows the reading from but not writing to the device.

3.8.8. Prohibit the use of portable storage devices when such devices have no identifiable owner.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC has established strict controls over the use of portable media. When an unidentified portable storage device is inserted into a NORC-owned, encrypted corporate device, WinMagic allows the reading from but not writing to the device.

3.8.9. Protect the confidentiality of backup CIPSEA Information at storage locations (e.g. FIPS 140-2 compliant encryption solutions).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- CIPSEIA Information will remain on NORC Disk arrays in their data centers. The data backups will remain on disk arrays hardware which are FIPS 140-2 compliant.

3.9. Personnel Security

3.9.1. Screen individuals prior to authorizing access to organizational systems containing CIPSEA Information.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC HR is responsible for determining the screening and re-screening requirements, conditions and frequencies. They are also responsible for ensuring screening and re-screening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position.
- Personnel screening for an individual prior to access in the information system is the responsibility of the NORC Human Resources (HR) department.
- Re-screening on the organizationally defined frequency is the responsibility of NORC's HR department. It is also the responsibility of the Project Director to contact NORC's ISO team and authorize the creation of the user account.

3.9.2. Ensure that organizational systems containing CIPSEA Information are protected during and after personnel actions such as terminations and transfers.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Employee are required to maintain their confidentiality of all NORC data regardless if they are actively on the project or employed at NORC.

Physical Protection

3.9.3. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All NORC facilities, access to datacenter and all infrastructure is protected by card readers. Only approved personnel are granted access to the datacenter and infrastructure wiring closets.

3.9.4. Protect and monitor the physical facility and support infrastructure for organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All NORC facilities doors are protected card readers. The facilities are monitored by security cameras. The facilities are wired with fire protection.
- The Zayo datacenter requires all users to show a valid government id. All doors are controlled by card readers. The facility has security cameras throughout the facility. The datacenter is equipped with full fire protection.
- The datacenter has full power protection using batteries and power generators.

3.9.5. Escort visitors and monitor visitor activity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All official visitors and service vendors are required to be escorted into the facility by designated personnel. They are required to log in at the reception desk when they arrive and log out when they leave the facility. Appropriate temporary badges may be assigned to visitors upon entering the facility and will be collected at their departure. Those visitors who may or will be exposed to NORC or sponsor information or data must sign a NORC Statement of Professional Ethics Form.

3.9.6. Maintain audit logs of physical access.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All Data Center Visitor Access Records must be retained by NORC ISO Engineering for a minimum of 3 years.
- NORC ISO Engineering, along with the ISO Director, reviews data center visitor logs on a quarterly basis to determine which non-NORC personnel have accessed the data center.

3.9.7. Control and manage physical access devices.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All access devices to the data center where CIPSEA data is stored is managed by our datacenter vendor Zayo. They maintain all access control card readers, video surveillance equipment and alarm systems.

3.9.8. In accordance with the DAA, no access to CIPSEA Information (e.g. sampling frame) is permitted from alternate work sites.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- This is a web survey. Respondents enter their responses over the Internet.
- No CIPSEA protected information will be accessed remotely as specified in the DAA.

3.10. Risk Assessment

3.10.1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CIPSEA Information.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC conducts an assessment of risk on the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from unauthorized access, use or disclosure.
- NORC documents risk assessment results in forms provided by the Federal Agencies it serves for each information system, on a project-specific basis, and limited by system boundaries. Specific information systems may also require the risk assessment results be documented in additional locations based on the contract.

3.10.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC scans for system vulnerabilities in its information systems, in hosted applications and when new vulnerabilities potentially affecting the system or application are identified and reported.
- Entire system scans are to be performed on a weekly basis. Application scans are to be performed at least quarterly.
- The ISO Team may run random, or on-demand system scans when new vulnerabilities are suspected or have been identified that may potentially affect the system.

3.10.3. Remediate vulnerabilities in accordance with risk assessments.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC remediates legitimate vulnerabilities in various timeframes in accordance with an organizational assessment of risk. NORC also shares information obtained from the vulnerability scanning process and security control assessments with designated personnel within NORC's IT Department to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
- All vulnerabilities rated Critical, High or Medium by the scanning tools must be addressed.

3.11. Security Assessment

3.11.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC has their controls review by external assessors at least annually

3.11.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC maintains a list active and completed POAM items from previous assessments.

3.11.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC reviews all security controls at least annually.
- NORC updates any security control when there is a significant change to the information system.

3.11.4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC maintains a separate System Security Plan for each project. Each project has a defined security boundary

3.12. System and Communications Protection

3.12.1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- The NORC external boundaries are protected by multiple firewalls. All traffic is logged and monitored.
- All emails are monitored as they enter the company boundary.

3.12.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- 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
- NORC Management factors information security concerns and regulatory compliance implications as part of every significant business decision.

3.12.3. Separate user functionality from system management functionality.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All administrators are given two accounts. A regular account and an administrator account. All user functionality is performed from their regular account. All administrator functions are performed with their administrator account.

3.12.4. Prevent unauthorized and unintended information transfer via shared system resources.

☐ Implemented ☐ Planned to be Implemented ☒ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- There are no shared system resources as part of this project.

3.12.5. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All web accessible systems are on their own subnet and are protected by multiple firewalls. The public address is protected from the Internet by a firewall. Access to the internal network is protected by a separate firewall.
- All internal servers are not publicly accessible from the Internet.

3.12.6. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide

rationale.

- The firewalls have a default deny all traffic. All traffic must be explicitly permitted.

3.12.7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC remove access does not allow split tunneling.
- If an application requires split tunneling it must be approved by the Information Security Officer.

3.12.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of CIPSEA Information during transmission unless otherwise protected by alternative physical safeguards.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All server connections and web access is protected by TLS encryption. All remote access traffic over SSL/TLS.

3.12.9. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- All session are terminated at end of the session.
- Session termination due to inactivity is defined in each application. Most application have a 30 minutes inactivity termination.

3.12.10. Establish and manage cryptographic keys for cryptography employed in organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC establishes and manages cryptographic keys for required cryptography employed within the information system. NORC follows NIST Special Publications 800-57 and 800-133 guidelines for cryptographic key establishment and management.
- Specifically NORC requires the following for cryptographic keys:

- 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 (e.g. RSA) and hashes (e.g. SHA2).
- • Proper lifecycle management of keys.
- • Proper key backup and recovery procedures.
-

3.12.11. Employ FIPS-validated cryptography when used to protect the confidentiality of CIPSEA Information.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC information systems must implement required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. NORC information systems employ FIPS 140-2 validated cryptographic algorithms and modules for the protection of sensitive or valuable data.

3.12.12. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC limits the use of collaborative computing software to Microsoft Skype for Business, TeamViewer and Remote Desktop Connection using Remote Desktop Protocol (RDP).
- NORC information systems must provide an explicit indication of use to users physically present at the devices. In both collaborative environments, the user initiating the session must be at their terminal. Sessions cannot be initiated on a client computer remotely without permission by the user. All collaborative computing devices used by NORC are equipped with indication lights which signal to users when these devices are in use.

3.12.13. Control and monitor the use of mobile code.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC defines two categories of mobile code in the information system, Category 1 and Category 2. Mobile code is software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient.
- The following Category 1 mobile code technologies are acceptable given they are with usage restrictions defined in Section 4.2 below:
  - ActiveX controls
- The following mobile code technologies are examples of acceptable Category 2 technologies.
  - Java applets

- Visual Basic for Applications
- PostScript
- JavaScript, when executing in the browser
- VBScript, when executing in the browser
- Portable Document Format (PDF)
- Flash

3.12.14. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC authorizes, monitors, and controls the use of Voice over Internet Protocol (VoIP) within the information system. To achieve this level of control and monitoring over its VoIP systems, NORC establishes usage restrictions and implementation guidance for VoIP technologies based on the potential damage that telephony systems could incur if such systems were used maliciously.
- VOIP is employed only for internal phone communications. Communications are monitored for misuse via reporting and billing information. NORC management also restricts the ability to make long distance calls utilizing filters.
- NORC authorizes, monitors and controls the use of VoIP within the information system. Call detail records are reviewed and charged to their specific projects, publicly accessible phones are configured for internal dialing only, and in order to place international calls, users must obtain approval to be added to a specific dialing group with such permissions.

3.12.15. Protect the authenticity of communications sessions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC implements session authenticity for communications where deemed necessary by NORC. Session authenticity is ensured through the use of transmission integrity and confidentiality methods defined NORC SOP IT-26 (SC-8), Transmission Integrity and NORC SOP IT-27 (SC-9), Transmission Confidentiality. Encryption is also used to provide authenticity of communication sessions when required. When encryption is used, it conforms to the requirements of NORC SOP IT-28 (SC-13), Use of Cryptography.

3.12.16. Protect the confidentiality of CIPSEA Information at rest by way of FIPS 140-2 compliant encryption solutions.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Data at rest is stored on encrypted hard drives.

3.13. System and Information Integrity

3.13.1. Identify, report, and correct system flaws in a timely manner.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC scans all servers with a SCAP compliance Nessus vulnerability scanner to identify system flaws. NORC reports on these scans on a weekly basis.
- NORC can scan any server on demand if needed.
- NORC remediates vulnerabilities within 1 to 30 days depending on the severity.

3.13.2. Provide protection from malicious code at designated locations within organizational systems.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC firewalls identifies and blocks malicious code from entering the NORC environment.
- NORC has email firewall which scan all emails for malicious code attachments.
- NORC runs McAfee EPO antivirus/antimalware software on all workstation and servers. The antivirus software will identify malicious code and remove it from the system automatically.
- NORC event log monitoring SIEM tool monitors logs for detection of malicious code.

3.13.3. Monitor system security alerts and advisories and take action in response.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC received security alerts and advisories from multiple sources.
  - Microsoft Security Alerts.
  - SANs alerts
  - Palo Alto security updates
  - US-Cert advisories
  - SearchSecurity

3.13.4. Update malicious code protection mechanisms when new releases are available.

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- NORC systems automatically receive system updates when they are available.
  - Palo Alto receives new threat signatures when they are available.
  - McAfee EPO antivirus signature updates
  - Barracuda Email firewall receives updates when they are available

3.13.5. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- McAfee EPO scans all new files in real-time for malicious software. McAfee also does periodic scan of the entire file system on a daily basis.

3.13.6. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Barracuda Email firewalls monitors all emails as they enter and leave the environment.
- Palo Alto firewalls identify threats and stops them at the firewall.

3.13.7. Identify unauthorized use of organizational systems.

☒ Implemented □ Planned to be Implemented □ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

- Users are not administrators on their machines and are not allowed to install unauthorized software.

4. RECORD OF CHANGES

Date	Description	Made By:
9/12/2023	Initial completion of Protection plan	C. Armstrong