Georgia Tech System Security Plan

GT SSP

Overview

This Standard System Security Plan (SSP) has been developed and will be used to protect all systems storing and processing CUI and thus requiring compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204.7012 *Safe Guarding Defense Information and Cyber Incident Reporting*.

Purpose

This document outlines the management, operational, and technical safeguards or countermeasures approved by the Institute for meeting the requirements for an information system or storage location/device involved with CUI. Deviations will be documented and will require the approval of the CISO and appropriate Executive Vice President or their designees.

Instructions

The Principal Investigator (PI), or designee, shall submit the SSP prior to the commencement of work for the project.

The Controls

The SSP NIST 800-171 Controls Form lists each control, the control family, the control text and the approved solution for each of the 110 controls. These approved solutions are offered as centrally supported services. In situations where the approved solution is not possible or appropriate for your system, the compliance team will work with you to identify an approved mitigation. All mitigations will be filed as a supplemental SSP to the standard SSP. Both will require the signature of the Principal Investigator. If utilizing an approved central solution, no action is needed.

Revision History

Name	Date	Description of Change	Version Number
Kyle Smith	08/15/2018	Document Creation	1.00
Kyle Smith	08/27/2018	Added Revision History	1.01
Kyle Smith	9/13/2018	NIST ROC Translation Changes Loaded Added table inside Users Involved List	1.02
Kyle Smith	9/18/2018	Approvals Complete. Transition to v2.00	2.00
Kyle Smith	9/19/2018	Adjusted 3.14.3, removed Splunk reference Adjusted 3.5.3 to remove automatic from control	2.00
Leon Blake	9/24/2018	Added Machine Type to System Inventory, Made Grammatical changes to Footnotes #10, #15, #16 and #28	2.01
Kyle Smith	9/25/2018	Adjusted table size on Systems Inventory	2.01
Kyle Smith	5/29/2019	Adjusted cloud services to reflect Office 365 and Box	2.05
Kyle Smith	6/27/2019	Major adjustments to controls and footnotes. Transition to v3.00.	3.00
Kyle Smith	9/25/2019	Small adjustment to control solutions and footnote	3.01

Contents

Project Summary

Please complete the information below.

Project Information

Prime Award Number			
Document ID			
Primary Sponsor			
Project Title			
Principal Investigator			
Name/Role of Users Working on This Project	***Full Name***	***Role***	***Login Accounts Used***
Physical Location(s)			
Project IT Contact			
Contracting Officer			

Description of research/work/project

Please describe the nature of the research being done, as well as some of the details at a high level, that will present a picture of how data is processed in this project.

Description of CUI

What CUI is involved in the project and how it will be handled? Make sure you address; CUI that is delivered to you from external sources, CUI you generate, and CUI you deliver to external sources**.**

Systems Inventory

Please complete an SSP Systems Inventory Sheet. This should include all information systems that will be used to handle CUI for this project

Ownership	Owner (Primary_User)	User Classification	Used for Data Acquisition?	Primary Location Building - Room	Machine Type	Hostname	MAC Address

NIST 800-171 Controls Form

For all deviations, or items where there is no approved central solution (marked None) an approved mitigation should be entered.

NIST 800-171 Control Number	Control Family	Control Text	Standard Solution	Project-Specific Solutions and Mitigations
3.1.1	Access Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Central Endpoint Management[1] GT-AMS[2]	
3.1.2	Access Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Central Endpoint Management GT-AMS	
3.1.3	Access Control	Control the flow of CUI in accordance with approved authorizations.	*(To be determined as appropriate per project)*	
3.1.4	Access Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	GT Employment Structure	
3.1.5	Access Control	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Central Endpoint Management GT-AMS	
3.1.6	Access Control	Use non-privileged accounts or roles when accessing nonsecurity functions.	Central Endpoint Management GT-AMS	
3.1.7	Access Control	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Central Endpoint Management GT-AMS	
3.1.8	Access Control	Limit unsuccessful logon attempts.	Central Endpoint Management GT-AMS	
3.1.9	Access Control	Provide privacy and security notices consistent with applicable CUI rules.	Central Endpoint Management	

[1] These tools comprise the centrally offered Endpoint Management Suite: System Center Configuration Manager - SCCM (Windows) JAMF (MacOS) SaltStack (Linux), and Georgia Tech's Active Directory infrastructure - GTAD and the GPOs centrally managed through that resource.

[2] Georgia Tech Account Management Services (GT-AMS) is a combination of policies and tools which enforce requirements around user accounts on campus and how those accounts interact with systems and services.

3.1.10	Access Control	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	Central Endpoint Management	
3.1.11	Access Control	Terminate (automatically) a user session after a defined condition.	*(To be determined as appropriate per project)*	
3.1.12	Access Control	Monitor and control remote access sessions.	GT VPN[3]	
3.1.13	Access Control	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	GT VPN	
3.1.14	Access Control	Route remote access via managed access control points.	GT VPN	
3.1.15	Access Control	Authorize remote execution of privileged commands and remote access to security-relevant information.	Central Endpoint Management	
3.1.16	Access Control	Authorize wireless access prior to allowing such connections.	GT Wireless[4]	
3.1.17	Access Control	Protect wireless access using authentication and encryption.	GT Wireless & GT VPN	
3.1.18	Access Control	Control connection of mobile devices.	GT Wireless & GT VPN	
3.1.19	Access Control	Encrypt CUI on mobile devices.	Bitlocker[5] FileVault[6] Linux LUKS[7]	
3.1.20	Access Control	Verify and control/limit connections to and use of external information systems.	Sponsor Portal	
3.1.21	Access Control	Limit use of organizational portable storage devices on external information systems.	*(To be determined as appropriate per project)*	

[3] Georgia Tech uses Cisco AnyConnect VPN which offers a 2FA option. All employees and students are required to use the 2FA option.
[4] GT Wireless is comprised of two SSIDs that are options for this SSP. Eduroam is the preferred Georgia Tech wireless offering. GTother may be used in situations where the preferred options cannot be used.
[5] BitLocker encryption uses AES to encrypt entire volumes on Windows server and client machines.
[6] Apple FileVault full-disk encryption (FileVault 2) uses XTS-AES-128 encryption with a 256-bit key to help prevent unauthorized access to the information on or from MacOS.
[7] LUKS is the standard for Linux hard disk encryption.

3.1.22	Access Control	Control information posted or processed on publicly accessible information systems.	*(To be determined as appropriate per project)*	
3.2.1	Awareness and Training	Ensure that managers, systems administrators, and users of organizational information 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 organizational information systems.	NARA CUI Training[8]	
3.2.2	Awareness and Training	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	NARA CUI Training	
3.2.3	Awareness and Training	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	NARA CUI Training	
3.3.1	Audit and Accountability	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	Central Endpoint Management, Local Settings[9], LMaaS[10] & Cloud Services Management[11]	
3.3.2	Audit and Accountability	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	Central Endpoint Management, GT-AMS, Local Settings, LMaaS, & Cloud Services Management	

[8] Georgia Tech Research Corporation (GTRC) is constructing the training that will be used for this purpose. In the meantime, training can be found on the Georgia Tech CUI webpage. cui.gatech.edu/cui_training

[9] Log settings can be configured locally on machines in-scope to make sure that appropriate actions are being logged, and that log file space on the client machine is managed to avoid issues. Local logging settings are valid for macOS, Windows, and Linux Operating Systems.

[10] Log Management as a Service (LMaaS) is a centrally provided service for the management of system logs from campus systems that have been configured to use export their logs to a log management platform monitored by Cyber Security.

[11] Cloud Services Management are services that offer management of files and folders with version history and vendor managed logs for protection. Appropriate service for use at Georgia Tech are located here: https://faq.oit.gatech.edu/content/which-cloud-storage-offering-should-i-use.

3.3.3	Audit and Accountability	Review and update audited events.	Central Endpoint Management, Local Settings, LMaaS, & Cloud Services Management	
3.3.4	Audit and Accountability	Alert in the event of an audit process failure.	Central Endpoint Management, Local Settings, LMaaS, & Cloud Services Management	
3.3.5	Audit and Accountability	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Central Endpoint Management, Local Settings, LMaaS, & Cloud Services Management	
3.3.6	Audit and Accountability	Provide audit reduction and report generation to support on-demand analysis and reporting.	Central Endpoint Management, Local Settings, LMaaS, & Cloud Services Management	
3.3.7	Audit and Accountability	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	GTAD & GT NTP[12]	
3.3.8	Audit and Accountability	Protect audit information and audit tools from unauthorized access, modification, and deletion.	Central Endpoint Management, GT-AMS, Local Settings, LMaaS, & Cloud Services Management	

[12] GT AD handles NTP services for domain joined machines. Georgia Tech also offers NTP servers for use. Information about Georgia Tech NTP servers is located here: https://faq.oit.gatech.edu/content/what-can-i-use-ntp-time-server.

3.3.9	Audit and Accountability	Limit management of audit functionality to a subset of privileged users.	Central Endpoint Management, Local Settings, LMaaS, & Cloud Services Management	
3.4.1	Configuration Management	Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Central Endpoint Management	
3.4.2	Configuration Management	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	Central Endpoint Management	
3.4.3	Configuration Management	Track, review, approve/disapprove, and audit changes to information systems.	Support Ticketing System[13]	
3.4.4	Configuration Management	Analyze the security impact of changes prior to implementation.	Support Ticketing System	
3.4.5	Configuration Management	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.	Support Ticketing System	
3.4.6	Configuration Management	Employ the principle of least functionality by configuring the information system to provide only essential capabilities.	Central Endpoint Management	
3.4.7	Configuration Management	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Central Endpoint Management & Support Ticketing System	

[13] The Configuration Management controls can be met if a ticketing system is used to track all major software install requests and any hardware changes outside of system repairs. All systems covered by an SSP must have these requests routed and approved through the ticket system to be compliant. The Georgia Tech Change Request Form can also be used for both ad hoc and recurring changes that may impact the security of the system.

3.4.8	Configuration Management	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Central Endpoint Management	
3.4.9	Configuration Management	Control and monitor user-installed software.	Central Endpoint Management & Support Ticketing System	
3.5.1	Identification and Authentication	Identify information system users, processes acting on behalf of users, or devices.	GT-AMS[14] & SSP Document	
3.5.2	Identification and Authentication	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	GT-AMS & SSP Document	
3.5.3	Identification and Authentication	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	GT 2FA[15] LastPass[16] Thycotic Secret Server[17]	
3.5.4	Identification and Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	GT 2FA	
3.5.5	Identification and Authentication	Prevent reuse of identifiers for a defined period.	GT-AMS Central Endpoint Management Local user identifiers are removed when drives are either sanitized for reuse or sent to GTRI Disposal Service[18]	

[14] Georgia Tech Account Management Services (GT-AMS) is a combination of policies and tools which enforce requirements around user accounts on campus and how those accounts interact with systems and services.
[15] GT 2FA (Georgia Tech Two-Factor Authentication) secures access to services where required.
[16] Georgia Tech offers LastPass to provide additional security when using privileged accounts accessed with Two-Factor Authentication.
[17] Georgia Tech offers Thycotic's Secret Server which uses Two-Factor Authentication to secure access to the password vault.
[18] Georgia Tech Research Institute (GTRI) provides the secure destruction of sensitive hardware media as a service.

3.5.6	Identification and Authentication	Disable identifiers after a defined period of inactivity.	GT-AMS Applicable local identifiers are disabled or removed when they are no longer active.	
3.5.7	Identification and Authentication	Enforce a minimum password complexity and change of characters when new passwords are created.	Central Endpoint Management	
3.5.8	Identification and Authentication	Prohibit password reuse for a specified number of generations.	Central Endpoint Management	
3.5.9	Identification and Authentication	Allow temporary password use for system logons with an immediate change to a permanent password.	Central Endpoint Management GT Employee Onboarding	
3.5.10	Identification and Authentication	Store and transmit only encrypted representation of passwords.	Central Endpoint Management GT-AMS Thycotic Secret Server LastPass	
3.5.11	Identification and Authentication	Obscure feedback of authentication information.	GT-AMS Operating System Default	
3.6.1	Incident Response	Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	Cyber Security[19] & Project IT[20]	
3.6.2	Incident Response	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.	Cyber Security & Project IT	
3.6.3	Incident Response	Test the organizational incident response capability.	Cyber Security & Project IT	

[19] Georgia Tech's Cyber Security Security Operations Center (SOC) acts as an escalation point for information security concerns for the campus. They are the responsible unit for all reporting and incident response related issues. The SOC can be contacted by calling 404.385.CYBR or emailing soc@gatech.edu.
[20] Project IT includes any IT staff that actively support the systems in-scope for NIST 800-171.

3.7.1	Maintenance	Perform maintenance on organizational information systems.	Not Applicable - No significant maintenance is required on in-scope systems	
3.7.2	Maintenance	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	Not Applicable - No significant maintenance is required on in-scope systems	
3.7.3	Maintenance	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Not Applicable - No significant maintenance is required on in-scope systems	
3.7.4	Maintenance	Check media containing diagnostic and test programs for malicious code before the media are used in the information system.	Not Applicable - No significant maintenance is required on in-scope systems	
3.7.5	Maintenance	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Not Applicable - No significant maintenance is required on in-scope systems	
3.7.6	Maintenance	Supervise the maintenance activities of maintenance personnel without required access authorization.	Not Applicable - No significant maintenance is required on in-scope systems	
3.8.1	Media Protection	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.	*(To be determined as appropriate per project)*	
3.8.2	Media Protection	Limit access to CUI on information system media to authorized users.	Central Endpoint Management SSP Document	

3.8.3	Media Protection	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	Drives are either sanitized for reuse or sent to GTRI Disposal Service	
3.8.4	Media Protection	Mark media with necessary CUI markings and distribution limitations.	In-scope physical media is labeled	
3.8.5	Media Protection	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	*(To be determined as appropriate per project)*	
3.8.6	Media Protection	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	*(To be determined as appropriate per project)*	
3.8.7	Media Protection	Control the use of removable media on information system components.	*(To be determined as appropriate per project)*	
3.8.8	Media Protection	Prohibit the use of portable storage devices when such devices have no identifiable owner.	*(To be determined as appropriate per project)*	
3.8.9	Media Protection	Protect the confidentiality of backup CUI at storage locations.	Dropbox[21] Office 365[22] Box[23]	
3.9.1	Personnel Security	Screen individuals prior to authorizing access to information systems containing CUI.	OHR[24]	
3.9.2	Personnel Security	Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Access to CUI is removed immediately upon termination or transfer from the project	

[21] Georgia Tech Dropbox Enterprise – please note that only Georgia Tech Box Accounts are compliant, and CUI must be encrypted first before it is stored in Dropbox.
[22] This is for the instance associated with Georgia Tech's Office 365 offering. Personal Office 365 accounts are noncompliant with established Georgia Tech Policies
[23] Georgia Tech Box Account – please note that only Georgia Tech Box Accounts are compliant.
[24] Georgia Tech Office of Human Resources

3.10.1	Physical Protection	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	BuzzCard Readers[25] Door Keys[26]	
3.10.2	Physical Protection	Protect and monitor the physical facility and support infrastructure for those information systems.	BuzzCard Readers Video Cameras[27] Door Keys	
3.10.3	Physical Protection	Escort visitors and monitor visitor activity.	Visitors are escorted at all times	
3.10.4	Physical Protection	Maintain audit logs of physical access.	BuzzCard Readers Video Cameras Door Keys	
3.10.5	Physical Protection	Control and manage physical access devices.	BuzzCard Readers Video Cameras Door Keys	
3.10.6	Physical Protection	Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).	*(To be determined as appropriate per project)*	
3.11.1	Risk Assessment	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	GT NIST 800-171 Process[28]	
3.11.2	Risk Assessment	Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	QEP[29]	
3.11.3	Risk Assessment	Remediate vulnerabilities in accordance with assessments of risk.	QEP	

[25] This is Georgia Tech's card reader-based door access system.
[26] Physical keys require the use of a key management and tracking system. This should be reviewed on a periodic basis.
[27] Georgia Tech's police department provides central monitoring for a network of video cameras across campus.
[28] GT NIST 800-171 Process includes this SSP as well as an assessment soon after. Assessment results are recorded on a Report on Compliance (ROC) to ensure the SSP is being upheld.
[29] Qualys Endpoint Agent (QEP) is an extension of campus's Qualys network scanning service that allows more complete information to be obtained for use with vulnerability assessment and system compliance with certain control requirements.

3.12.1	Security Assessment	Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	GT NIST 800-171 Process	
3.12.2	Security Assessment	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.	GT NIST 800-171 Process	
3.12.3	Security Assessment	Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	LMaaS & Central Endpoint Management GT NIST 800-171 Process	
3.12.4	Security Assessment	Develop, document, periodically update, and implement system security plans for organizational information systems that describe the security requirements in place or planned for the systems.	GT NIST 800-171 Process	
3.13.1	System and Communications Protection	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Palo Alto NGFW	
3.13.2	System and Communications Protection	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	*(To be determined as appropriate per project)*	
3.13.3	System and Communications Protection	Separate user functionality from information system management functionality.	Central Endpoint Management	
3.13.4	System and Communications Protection	Prevent unauthorized and unintended information transfer via shared system resources.	*(To be determined as appropriate per project)*	
3.13.5	System and Communications Protection	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Not Applicable - Publicly accessible systems are not used	

3.13.6	System and Communications Protection	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Palo Alto NGFW	
3.13.7	System and Communications Protection	Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.	GT VPN	
3.13.8	System and Communications Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Dropbox Office 365 Box GT VPN	
3.13.9	System and Communications Protection	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	*(To be determined as appropriate per project)*	
3.13.10	System and Communications Protection	Establish and manage cryptographic keys for cryptography employed in the information system;	*(To be determined as appropriate per project)*	
3.13.11	System and Communications Protection	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Dropbox Office 365 Box Bitlocker[30] FileVault[31] Linux LUKS[32] GT VPN	
3.13.12	System and Communications Protection	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	BlueJeans[33] Skype for Business[34] WebEx[35] Microsoft Teams[36]	

[30] All versions of BitLocker must be configured for FIPS 140-2 compliance.
[31] FileVault is generally FIPS validated. Apple maintains current status of FIPS 140-2 validation on their website.
[32] LUKS is FIPS 140-2 compliant by default when employed by a RHEL machine. All other Linux installations using LUKS require additional configuration to be FIPS 140-2 compliant.
[33] Georgia Tech BlueJeans Collaboration
[34] Skype for Business is available through Office 365
[35] Georgia Tech WebEx Collaboration
[36] Microsoft Teams is available through Office 365

3.13.13	System and Communications Protection	Control and monitor the use of mobile code.	Not Applicable - Mobile Code is not used	
3.13.14	System and Communications Protection	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	BlueJeans Skype for Business WebEx Microsoft Teams	
3.13.15	System and Communications Protection	Protect the authenticity of communications sessions.	Palo Alto NGFW	
3.13.16	System and Communications Protection	Protect the confidentiality of CUI at rest.	Dropbox Office 365 Box Bitlocker FileVault Linux LUKS	
3.14.1	System and Information Integrity	Identify, report, and correct information and information system flaws in a timely manner.	Central Endpoint Management Support Ticketing System	
3.14.2	System and Information Integrity	Provide protection from malicious code at appropriate locations within organizational information systems.	FireEye Agent[37] Palo Alto NGFW	
3.14.3	System and Information Integrity	Monitor information system security alerts and advisories and take appropriate actions in response.	SOC[38] and Project IT	
3.14.4	System and Information Integrity	Update malicious code protection mechanisms when new releases are available.	FireEye Agent	

[37] FireEye HX is the agent based, centrally offered and managed antimalware tool (not available for Ubuntu)
[38] SOC (System Operations Center) is the area of Cyber Security that handles first tier Security Incidents

3.14.5	System and Information Integrity	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	FireEye Agent	
3.14.6	System and Information Integrity	Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	LMaaS & Palo Alto NGFW	
3.14.7	System and Information Integrity	Identify unauthorized use of the information system.	LMaaS & Palo Alto NGFW	

Plans of Action and Milestones (POA&Ms)

For any of the NIST 800-171 requirements that are not met, a POA&M is required. List these POA&Ms below and add additional rows as needed.

Control Number	Control Description	Remediation plan	Due Date

Barriers to Compliance

For any of the NIST 800-171 requirements that are not currently met, list all barriers to compliance. These could include lack of funding for a specific type of control, lack of personnel necessary to perform necessary tasks and duties, etc. Provide a cost estimate of what would be required to remove these barriers. Do not count costs multiple times if they apply to multiple requirements, instead reference the control number where the cost is already accounted for. Add additional rows as needed.

Control Number	Control Description	Barriers to Compliance	Cost Estimate

Approvals

I acknowledge that I will manage CUI associated with this project in accordance with this SSP.

Principal Investigator (printed): _____

Principal Investigator (signature):

_____

Approval Date: _____

Approved CISO or Designee (printed) _____

Approved CISO or designee (signature)

_____

Approval Date _____

Approved VP Research or Designee (printed) _____

Approved VP Research or Designee (signature)

_____

Approval Date _____

SSP is valid for one year after the date that Principal Investigator signs the document.

END OF DOCUMENT