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 sensitive data and thus requiring compliance to the safeguards of NIST 800-171.

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 sensitive data. Deviations will be documented and will require the approval of the CISO.

Instructions

The Principal Investigator, or designee, shall submit the SSP prior to saving sensitive data to, processing sensitive data with, or sending sensitive data from the lab or environment.

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 systems, 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	11/5/2019	Document Creation	1.00
Kyle Smith	2/14/2020	Update to include GT-AMS for 3.5.7-9, Central Endpoint Management for 3.7.1-2, and add Machine Type to System Inventory	2.00
Kyle Smith	4/1/2020	Update to reflect control language in NIST 800-171 Rev 2	3.00
Kyle Smith	8/4/2020	Updating to add MPT Ref Number and SSP Version Number. Other updates are in process, so this isn't a full version change.	3.05
Kyle Smith	9/9/2020	Added DFARS 7012 C-G controls as well as "Updates from previous SSP box" and an initial for when GTRC IT reviews an SSP and ROC.	4.00

Contents

Environment/Lab Summary

Please complete the information below.

Environment/Lab Information

Lab/Environment General Title			
MPT Reference Number		**SSP Version Number**	
Principal Investigator			
Name/Role of Users Working in this Lab/Environment	***Full Name***	***Email Address***	***Login Accounts Used***
Physical Location(s)	Location Name:	Location Address(es):	
Primary IT Contact			

Flow Diagram

Description of Environment/Lab

Please describe the nature of the Environment/Lab, as well as some of the details at a high level, that will present a picture of how data is processed.

Description of Sensitive Data

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

Changes from Previous SSP

If this is an update to a previous SSP, please list any changes made since the last iteration of the applicable SSP. If this is a new SSP, please enter “Not Applicable” in the box below.

Systems Inventory

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

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	Lab/Environment-Specific Solutions and Mitigations
3.1.1	Access Control	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Central Endpoint Management[1] GT-AMS[2]	
3.1.2	Access Control	Limit 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 sensitive data in accordance with approved authorizations.	*(To be determined as appropriate per lab/environment)*	
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 capture the execution of such functions in audit logs.	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 sensitive data rules.	Central Endpoint Management	
3.1.10	Access Control	Use session lock with pattern-hiding displays to prevent access and viewing of data after a 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 lab/environment)*	

[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.

3.1.12	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 sensitive data on mobile devices and mobile computing platforms.	Bitlocker[5] FileVault[6] Linux LUKS[7]	
3.1.20	Access Control	Verify and control/limit connections to and use of external systems	Sponsor Portal	
3.1.21	Access Control	Limit use of portable storage devices on external systems.	*(To be determined as appropriate per lab/environment)*	
3.1.22	Access Control	Control sensitive data posted or processed on publicly accessible systems.	*(To be determined as appropriate per lab/environment)*	

[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.

3.2.1	Awareness and Training	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.	NARA CUI Training[8]	
3.2.2	Awareness and Training	Ensure that personnel are 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 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.	Central Endpoint Management, Local Settings[9], LMaaS[10] & Cloud Services Management[11]	
3.3.2	Audit and Accountability	Ensure that the actions of individual 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	
3.3.3	Audit and Accountability	Review and update logged events	Central Endpoint Management, Local Settings, LMaaS, & Cloud Services Management	
3.3.4	Audit and Accountability	Alert in the event of an audit logging process failure	Central Endpoint Management, 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 sensitive data 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.

3.3.5	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 record 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 a 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 logging tools from unauthorized access, modification, and deletion.	Central Endpoint Management, GT-AMS, Local Settings, LMaaS, & Cloud Services Management	
3.3.9	Audit and Accountability	Limit management of audit logging 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 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 systems.	Central Endpoint 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.

3.4.3	Configuration Management	Track, review, approve or disapprove, and log changes to organizational 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 organizational systems.	Support Ticketing System	
3.4.6	Configuration Management	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Central Endpoint Management	
3.4.7	Configuration Management	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Central Endpoint Management & Support Ticketing System	
3.4.8	Configuration Management	Apply deny-by-exception (BlockListing) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (AllowListing) 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 system users, processes acting on behalf of users, and devices.	GT-AMS & SSP Document	
3.5.2	Identification and Authentication	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	GT-AMS & SSP Document	

[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.

3.5.3	Identification and Authentication	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	GT 2FA[14] LastPass[15] Thycotic Secret Server[16]	
3.5.4	Identification and Authentication	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged 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[17]	
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.	GT-AMS Central Endpoint Management	
3.5.8	Identification and Authentication	Prohibit password reuse for a specified number of generations.	GT-AMS Central Endpoint Management	
3.5.9	Identification and Authentication	Allow temporary password use for system logons with an immediate change to a permanent password.	GT-AMS Central Endpoint Management GT Employee Onboarding	
3.5.10	Identification and Authentication	Store and transmit only cryptographically-protected 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	

[14] GT 2FA (Georgia Tech Two-Factor Authentication) secures access to services where required.
[15] Georgia Tech offers LastPass to provide additional security when using privileged accounts accessed with Two-Factor Authentication.
[16] Georgia Tech offers Thycotic's Secret Server which uses Two-Factor Authentication to secure access to the password vault.
[17] Georgia Tech Research Institute (GTRI) provides the secure destruction of sensitive hardware media as a service.

3.6.1	Incident Response	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Cyber Security[18] & System IT[19]	
3.6.2	Incident Response	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Cyber Security & System IT	
3.6.3	Incident Response	Test the organizational incident response capability.	Cyber Security & System IT	
DFARS 7012 (c)(1)(i)[20]	Incident Response	**Cyber incident reporting requirement.** When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support.	Incident reporting requirements are detailed in Georgia Tech's incident response plan detailed here: https://gatech.service-now.com/kb_view.do?sysparm_article=KB0011532	

[18] 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.

[19] System IT includes any IT staff that actively support the systems in-scope for NIST 800-171.

[20] While not part of the NIST 800-171 control set, Georgia Tech includes sections (c)-(g) of DFARS 252.204-7012 to ensure that Incident Reporting Procedures are accounted for in conjunction with the controls of Control Family 3.6.

DFARS 7012 (c)(1)(ii)	Incident Response	**Cyber incident reporting requirement.** When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall rapidly report cyber incidents to DoD at https://dibnet.dod.mil.	Incident reporting requirements are detailed in Georgia Tech's incident response plan detailed here: https://gatech.service-now.com/kb_view.do?sysparm_article=KB0011532	
DFARS 7012 (c)(2)	Incident Response	**Cyber incident report.** The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.	Georgia Tech Cyber Security SOC (Security Operations Center) does not currently maintain a template for DoD incident reports; however, they follow the guidelines specified at https://dibnet.dod.mil.	
DFARS 7012 (c)(3)	Incident Response	**Medium assurance certificate requirement.** In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.	Georgia Tech Cyber Security SOC (Security Operations Center) has certificates registered during May 2018 and valid until May 2021.	
DFARS 7012 (d)	Incident Response	**Malicious software.** When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.	Incident response process includes acquisition of relevant artifacts, including malware samples that can be shared with DC3.	
DFARS 7012 (e)	Incident Response	**Media preservation and protection.** When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.	During security incidents, disk images are preserved as are all available network artifacts. Applicable network artifacts are collected and preserved as possible, as network artifacts may be limited based on date of incident identification and infrastructure limitations.	
DFARS 7012 (f)	Incident Response	**Access to additional information or equipment necessary for forensic analysis.** Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.	All artifacts for a forensic analysis when an incident is reported are preserved and available upon request.	

DFARS 7012 (g)	Incident Response	**Cyber incident damage assessment activities.** If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.	Georgia Tech Cyber Security SOC (Security Operations Center) conducts a financial impact assessment as part of the incident response process.	
3.7.1	Maintenance	Perform maintenance on organizational systems	Central Endpoint Management	
3.7.2	Maintenance	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Central Endpoint Management	
3.7.3	Maintenance	Ensure equipment removed for off-site maintenance is sanitized of any sensitive data.	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 organizational systems.	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) system media containing sensitive data, both paper and digital	*(To be determined as appropriate per lab/environment)*	
3.8.2	Media Protection	Limit access to sensitive data on system media to authorized users.	Central Endpoint Management SSP Document	
3.8.3	Media Protection	Sanitize or destroy system media containing sensitive data 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 sensitive data markings and distribution limitations	In-scope physical media is labeled	
3.8.5	Media Protection	Control access to media containing sensitive data and maintain accountability for media during transport outside of controlled areas.	*(To be determined as appropriate per lab/environment)*	

3.8.6	Media Protection	Implement cryptographic mechanisms to protect the confidentiality of sensitive data stored on digital media during transport unless otherwise protected by alternative physical safeguards.	*(To be determined as appropriate per lab/environment)*	
3.8.7	Media Protection	Control the use of removable media on system components.	*(To be determined as appropriate per lab/environment)*	
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 lab/environment)*	
3.8.9	Media Protection	Protect the confidentiality of backup sensitive data at storage locations.	GT Approved Cloud Services[21]	
3.9.1	Personnel Security	Screen individuals prior to authorizing access to organizational systems containing sensitive data.	OHR[22]	
3.9.2	Personnel Security	Ensure that organizational systems containing sensitive data are protected during and after personnel actions such as terminations and transfers.	Access to sensitive data is removed immediately upon termination or transfer from the system	
3.10.1	Physical Protection	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	BuzzCard Readers[23] Door Keys[24]	
3.10.2	Physical Protection	Protect and monitor the physical facility and support infrastructure for organizational systems.	BuzzCard Readers Video Cameras[25] Door Keys	
3.10.3	Physical Protection	Escort visitors and monitor visitor activity.	Visitors are escorted at all times	

[21] GT Approved Cloud Service include the services found on this page: https://faq.oit.gatech.edu/content/which-cloud-storage-offering-should-i-use (Note: ITAR, EAR, and CUI may be placed in Dropbox must be encrypted first before saving into the service).
[22] Georgia Tech Office of Human Resources
[23] This is Georgia Tech's card reader-based door access system.
[24] Physical keys require the use of a key management and tracking system. This should be reviewed on a periodic basis.
[25] Georgia Tech's police department provides central monitoring for a network of video cameras across campus.

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 sensitive data at alternate work sites.	*(To be determined as appropriate per lab/environment)*	
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 systems and the associated processing, storage, or transmission of sensitive data.	GT NIST 800-171 Process[26]	
3.11.2	Risk Assessment	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	QEP[27]	
3.11.3	Risk Assessment	Remediate vulnerabilities in accordance with risk assessments.	QEP	
3.12.1	Security Assessment	Periodically assess the security controls in organizational 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 systems.	GT NIST 800-171 Process	
3.12.3	Security Assessment	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	LMaaS & Central Endpoint Management GT NIST 800-171 Process	

[26] 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.

[27] 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.

3.12.4	Security Assessment	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.	GT NIST 800-171 Process	
3.13.1	System and Communications Protection	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.	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 systems.	*(To be determined as appropriate per lab/environment)*	
3.13.3	System and Communications Protection	Separate user functionality from 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 lab/environment)*	
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 organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	GT VPN	
3.13.8	System and Communications Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure of sensitive data during transmission unless otherwise protected by alternative physical safeguards.	GT Approved Cloud Services 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 lab/environment)*	

3.13.10	System and Communications Protection	Establish and manage cryptographic keys for cryptography employed in organizational system.	*(To be determined as appropriate per lab/environment)*	
3.13.11	System and Communications Protection	Employ FIPS-validated cryptography when used to protect the confidentiality of sensitive data.	GT Approved Cloud Services Bitlocker[28] FileVault[29] Linux LUKS[30] 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[31] Skype for Business[32] WebEx[33] Microsoft Teams[34]	
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 sensitive data at rest.	GT Approved Cloud Services Bitlocker FileVault Linux LUKS	

[28] All versions of BitLocker must be configured for FIPS 140-2 compliance.
[29] FileVault is generally FIPS validated. Apple maintains current status of FIPS 140-2 validation on their website.
[30] 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.
[31] Georgia Tech BlueJeans Collaboration
[32] Skype for Business is available through Office 365
[33] Georgia Tech WebEx Collaboration
[34] Microsoft Teams is available through Office 365

3.14.1	System and Information Integrity	Identify, report, and correct 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 designated locations within organizational systems.	FireEye Agent[35] Palo Alto NGFW	
3.14.3	System and Information Integrity	Monitor system security alerts and advisories and take action in response.	SOC[36] and System IT	
3.14.4	System and Information Integrity	Update malicious code protection mechanisms when new releases are available.	FireEye Agent	
3.14.5	System and Information Integrity	Perform periodic scans of organizational systems 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 organizational systems, 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 organizational systems.	LMaaS & Palo Alto NGFW	

[35] FireEye HX is the agent based, centrally offered and managed antimalware tool

[36] SOC (System Operations Center) is the area of Cyber Security that handles first tier Security Incidents

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 sensitive data associated with this Lab/Environment in accordance with this SSP.

Principal Investigator (printed): _____

Principal Investigator (signature):

_____

Approval Date: _____

CISO or Designee (printed) _____

CISO or Designee (signature)

_____

Approval Date _____

Reviewed by GTRC IT Team (Initial) _____

VP for Research or Designee (printed) _____

VP for Research or Designee (signature)

_____

Approval Date _____

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

END OF DOCUMENT