Intelligent Ground Vehicle Competition 2019
Cyber Challenge Report

Centaur

Delhi Technological University

May 18th 2019

Faculty Advisor Statement: I hereby certify that the development of vehicle, described in this report is original and has been equivalent to the work involved in a senior design course. This report has been prepared by the students of team Centaur under my guidance.

Dr. S. Indu
Department of Electronics and Communications Engineering, DTU

1. Team Member Details

Team Member	**Email Address**
Apoorv Goel (Captain)	apoorvgoel_bt2K16@dtu.ac.in
Robin K. Singh	robinvishen@gmail.com
Sudhanshu Shekhar Singh	singhsudhanshu204@gmail.com
Arindaam Roy	alpharoy14@gmail.com
Mukesh Yadav	mukesh7541@gmail.com
Sahil Jain	314sahil@gmail.com
Khwaish Kumar Anjum	kka011098@gmail.com
Manish Bhatia	manish4291@gmail.com
Sahil	sahil5051.ss@gmail.con
Parth Dharmarha	pddharmarha@gmail.com
Yashodhan Srivastava	yashodhansrivastava9@gmail.com
Samvandha Dev Pathak	psamvandha@gmail.com
Kshitij Rastogi	kshitij2301rastogi@gmail.com
Yatharth Ahuja	yatharthahuja1999@gmail.com
Nishant Kumar	kn1990kn@gmail.com
Jalan Ishu Kamal	ishujalan123@gmail.com

2. Understanding of the NIST RMF Process

Overview of NIST RMF process

- **Categorize** - This step is all administrative and involves gaining an understanding of the organisation. Prior to categorisation a system boundary should be defined. Based on that system boundary, all information type associated with the system can and should be identified. These information types include the information processed, stored, transmitted or protected by the information system. Information about the organisation and its mission, its roles and responsibilities as well as the system's operating environment, intended use and connection with other systems may affect the final security impact level determined for the information system.

  The information owner/information system owner identifies the types of information associated with the information system and assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability to each information type.

  References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-59, 800-60; CNSS Instruction 1253.

- **Select** - Security controls are the management, operational and technical safeguard or countermeasures employed within an organisational information system that protects the confidentiality, integrity and availability of the system and its information. Assurance boosts confidence in the fact that the security controls implemented within an information system are effective in their application.

  It is a two step process:

  1. Select the initial security control set.
  2. Taylor the initial security control.

References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-53, 800-53A; CNSS Instruction 1253.

- **Implement** - This step requires an organisation to implement security controls and describe how the controls are employed within the information system and its environment of operation. Policies should be tailored to each device to align with the required security documentation.

References: FIPS Publication 200; NIST Special Publications 800-30, 800-53, 800-53A; CNSS Instruction 1253.

- **Assess** - Assessing the security controls requires using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.

  References: NIST Special Publication 800-53A, 800-30, 800-70.

- **Authorize** - The authorize information system operation is based on a determination of the risk to organizational operations and individuals, assets, other organizations and the nation resulting from the operation of the information system and the decision that this risk is acceptable. Use reporting is designed to work with Plan of Action & Milestones. This provides the tracking and status for any failed controls.

  References: NIST Special Publications 800-30, 800-39, 800-53A.

- **Monitor** - Continuous monitoring programs allow an organization to maintain the security authorization of an information system over time in a highly dynamic operating environment where systems adapt to changing threats, vulnerabilities, technologies and mission/business processes. While the use of automated support tools is not required, risk management can become near real-time through the use of automated tools. This will help with configuration drift and other potential security incidents associated with unexpected change on different core components and their configurations.

  References: NIST Special Publications 800-30, 800-39, 800-53A, 800-53, 800-137; CNSS Instruction 1253.

Identified threat concept

- **Military Robotic Patrol** - The robot is part of a mission to protect a forward operating base (FOB) in Southwest Asia. It is a hot, empty desert environment surround by various sized sand dunes. The FOB is considered to be basic and temporary, and therefore consists of an arrangement of tents that serve various functions (including a hospital, a machine shop, and sleeping quarters) and a large open space to park ground vehicles and other similar systems.

The FOB is under constant threat of attack by enemy forces, and is therefore protected by a ring of barbed wire with a fortified entry control point, and sentries (mounted and dismounted) in key tactical locations. The robot is part of a team of robots tasked with autonomously patrolling the FOB perimeter to detect intrusions. The robots are not weaponized and only serve to provide early warning to the sentries of an imminent attack. The robots may also patrol areas around the perimeter that are out of the sentry line-of-sight, during daytime and nighttime, and be out of communication range for brief periods of time.

Thorough threat modelling

A. ***Security category vs security impact level***

A security category is the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations and assets, individuals, other organizations, or the Nation. Both information types and information systems have security categories—each with three components (one for each security objective) with a value of low, moderate, or high. However, an information system also has a security impact level, which consists of a single component with the value of low, moderate, or high. The security impact level for an information system is determined by taking the maximum impact value of the system’s security category. For a NSS, instead of taking just the maximum impact value, all designated impact values of confidentiality, integrity and availability are taken.

References WEB: csrc.nist.gov, FIPS Publications 199, 200.

B. ***Info needed to categorize an information system -***

Prior to categorizing a system, the system boundary should be defined. Based on the system boundary, all information types associated with the system can be identified. These information types include the information processed, stored, transmitted or protected by the information system. Information about the organization and its mission, as well as the system’s operating environment, intended use, and connections with other systems may affect the final security impact level determined for the information system. For example, if a system is connected to another system with a higher security impact level, it may be necessary to categorize the system at that higher impact level.

References WEB: csrc.nist.gov, FIPS Publication 199; NIST Special Publications 800-30, *800-39, 800-59, 800-60; CNSS Instruction 1253.*

C. *Information system boundaries*

The information system boundary is a logical group of information resources (information and related resources such as personnel, equipment, funds, and information technology) that have the same function or mission objectives, reside in the same general operating environment, and are under the same direct management control. It can be seen as a point where one's administrative control end and someone else's administrative control begins.

References WEB csrc.nist.gov.

D. *Types of information process by information systems*

Information is divided into two major categories—information associated with an organization's mission-specific activities and information associated with the administrative, management, and support activities common to most organizations.

Mission-based information types are, by definition, specific to individual organizations or groups of organizations and are the primary source for determining the security impact values and security objectives for mission-based information and information systems. The consequences or impact of unauthorized disclosure of information, breach of integrity, and denial of services are defined by the nature and beneficiary of the service being provided or supported.

Much of an organization's information and supporting information systems are not used to provide direct mission-based services but primarily to support the delivery of services or to manage resources.

Identification and mapping of cyber controls to counter identified threats

A. *Defense-in-depth*

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. An ideal defense-in-depth posture is 'deep', containing many layers of security, and 'narrow', the number of node independent attack paths is minimized.

B. *Technology based controls*

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

C. *Management and operational controls*

OPERATIONAL controls: The security controls for an information system that primarily are implemented and executed by people (as opposed to systems).
MANAGEMENT controls: The security controls for an information system that focus on the management of risk and the management of information system security.

D. *Security policies*

For an organization, it addresses the constraints on behaviour of its members. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

E. *Holistic approach to information security*

The NIST RMF has a holistic approach to a cyber security program by providing a framework core consisting of six functions (Categorize, Select, Implement, Authorize and Monitor), and includes guidelines, desired outcomes, and applicable references.

3. NIST RMF Process Applied to Competition Robot

Description of implemented cyber controls

A. Risks mitigated by the chosen controls

Controls	***Mitigated risk***
AC-2 Account management AC-2(2) Removal of temporary / Emergency accounts AC-2(5) Inactivity Logout AC-2(7) Role-based Schemes AC-2(13) Disable Accounts for High-Risk Individual	Spilling, mishandling of sensitive information by authorised or unauthorised users.
AC-3 Access Enforcement	Unauthorized logical access to information and system resources.
AC-4 Information Flow Enforcement	Untrusted flow of information within the system and interconnected system and connections with untrusted devices.
AC-5 Separation of Duty	Insider Threat. Malevolent activity without collusion such as tampering configuration of critical functions.
AC-6 Least Privilege AC-6(1) Authorize Access To Security Functions AC-6(2) Non-Privileged Access For Nonsecurity Functions AC-6(8) Privilege Level For Code Execution AC-6(9) Auditing The Use Of Privileged Functions AC-6(10) Prohibit Non Privileged Users from Executing Privileged Functions	Insider privilege misuse or abuse.
AC-8 System Use Notification	Access abuse.
AC-11 Session Lock AC-11(1) Pattern-Hiding Display	Unauthorized access to system information and system resources.
AC-12 Session Termination	Unauthorized access to system information and system resources.

AC-12(1) User-initiated Logouts/ Message Displays	
AC-17 Remote Access AC-17(1) Automated Monitoring AC-17(2) Protection of Confidentiality/ Integrity Using Encryption AC-17(9) Disconnect / Disable Access	Unauthorized access to system information and system resources. Preventing hostile systems from getting remote access. Sniffing of data over the network.
AC-18 Wireless Access AC-18(1) Authentication and Encryption AC-18(4) Restrict Configuration By Users	Network access to unauthorized individuals
AC-19 Access Control For Mobile Device	Malicious code infection. Unauthorized access to system information and resources from hostile sources.
AT-2 Security Awareness Training	Humans are the weakest link in security.
AU-3 Content of Audit Record	Loopholes in configuration of system.
AU-8 Time Stamps AU-8(1) Synchronization With Authoritative Sources	Inconsistency in real time.
AU-9 Protection of Audit Information AU-9(4) Access By Subset of Privileged users	Tampering of audit information.
AU-11 Audit Record Retention	Exploitation of unknown vulnerabilities
AU-12 Audit generation AU-12(3) Changes By Authorized Individual	Exploitation of unknown vulnerabilities
CA-3 System Interconnection CA-3(2) Classified National Security System Connections CA-3(5) Restriction on External Network Connections	Unauthorized access to system information and system resources.
CM-7 Least Functionality	System compromise as a virtue of large attack Surface.
CM-8 Information System Component Inventory	
CM-11(2) User Installed Software | Prohibit Installation Without Privileged Status	Installation of malicious softwares by unauthorised users.

CP-2(3) Contingency Plan | Resume Essential Mission Functions	High downtime of the system in case of faults in new versions of the system or malware attacks or any other contingency.
CP-10 Information System Recovery and Reconstruction	High downtime of the system in case of faults in new versions of the system or malware attacks or any other contingency.
IA-2 Identification And Authentication IA-2(1) Network Access To privileged Accounts IA-2(2) Network Access to Non privileged Accounts	Unauthorized access to system information and system resources.
IA-3 Device Identification and Authentication	Unauthorized access to system information and system resources from unknown devices.
IA-4 Identifier Management	Unauthorized access to system information and system resources.
IA-5 Authenticator Management IA-5(1) Password Based Authentication IA-5(2) PKI Based Authentication IA-5(4) Automated Support For Password Strength Determination IA-5(7) No Embedded Unencrypted Static Authenticators	Unauthorized access to system information and system resources.
IA-6 Authenticator Feedback	Eavesdropping resisting in compromization in confidentiality.
IR-5 Incident Monitoring	High system down time.
IR-6 Incident Reporting	High System Down time.
MA-4 Nonlocal Maintenance MA-4(6) Cryptographic Protection	Unauthorized access to system information and system resources.
PE-9 Power Equipment and Cabling	Damage and destruction to cables resulting in system down time.
PE-10 Emergency Shut Off	Damage to property or others.
PE-14 Temperature and Humidity Control	Overheating due to hot and humid conditions
PL-2 Security System Plan	Best Practices
RA-2 Security Categorization	In support of PL-2
SC-5 Denial Of Service Protection	Denial of Service

SC-7 Boundary Protection SC-7(5) Deny by Default/ Allow By Exception SC-7(11) Restrict Incoming Communicational Traffic SC-7(12) Host Based Protection	Best Practices
SC-8 Transmission Confidentiality and Integrity SC-8(1) Cryptographic or Alternate Physical	Compromized Confidentiality.
SC-10 Network Disconnect	
SC-12 Cryptographic Key establishment and Management	Unauthorized access to system information and system resources.
SC-17 Public Key Infrastructure Certificates	Unauthorized access to system information and system resources.
SI-3 Malicious Code Protection	Malware causing loss of confidentiality, integrity or availability of service.
SI-4 Information System Monitering	High System Down time.

B. Design and Implementation Details of Controls

Control	*Implementation*
AC-2 Account management	Installed CentOS in a virtual machine. Created different user accounts.
AC-2(2) Removal of temporary / Emergency accounts	While creating a user account, added an expiration date of the account.
AC-2(5) Inactivity Logout	Set the TMOUT variable to desired value in the .bash_profile file of the user accounts.
AC-2(7) Role-based Schemes	Added the users with administrative privileges to the group Wheel. This way the users can use the command sudo.
AC-2(13) Disable Accounts for High-Risk Individual	Root account was disabled. To use administrative privileges the user must use the sudo command.
AC-3 Access Enforcement	passwords were set for the user accounts.

AC-4 Information Flow Enforcement	Configured the firewall service to only accept connection to the different services from known / trusted systems. Implemented public key authentication for the user accounts over ssh protocol. The connection over ssh is encrypted.
AC-5 Separation of Duty	Configured Access Control List (ACL) for the user accounts depending on their duties.
AC-6 Least Privilege	Accounts were not given root privileges if not necessary. ACL was set accordingly.
AC-6(1) Authorize Access To Security Functions	Only the users who can use sudo can configure security functions.
AC-6(2) Non-Privileged Access For Nonsecurity Functions	A non privileged account was also made for system administrators.
AC-6(8) Privilege Level For Code Execution	Root account is never used for setting SUID for any code.
AC-6(9) Auditing The Use Of Privileged Functions	Find command is used to find all the file with SUID (privilege escalation) and also configured the Lynis tool to audit for privilege escalation.
AC-6(10) Prohibit Non Privileged Users from Executing Privileged Functions	Non privileged user accounts cannot execute privileged functions.
AC-8 System Use Notification	A system use banner was set by editing /etc/mybanner file and set the banner path in /etc/ssh/sshd_config.
AC-11 Session Lock AC-11(1) Pattern-Hiding Display	When physically accessing the system, after a certain period inactivity (say 120 seconds) the session of the user gets locked and the display gets masked.
AC-12 Session Termination	Session terminated after a certain time of inactivity which is configured in .bash_profile.
AC-12(1) User-initiated Logouts/ Message Displays	A logout message
AC-17 Remote Access	Configured OpenSSH service on the UGV system OS. Configured firewall to allow the service.

	Any system with a OpenSSH client and the right credentials can remotely connect to the robot system.
AC-17(1) Automated Monitoring	Configured the Monit tool to monitor ssh service.
AC-17(2) Protection of Confidentiality/ Integrity Using Encryption	Communication over ssh is encrypted.
AC-17(9) Disconnect / Disable Access	Remote access of users can be disables by configuring the /etc/ssh/ssh_config file.
AC-19 Access Control For Mobile Device	Configured firewall. Disabled unnecessary hardwares, ports, services. Installed the CalmAV tool for malware scanning.
AU-3 Content of Audit Record AU-12 Audit generation	Installed and configured Auiditd service for CentOS.
AU-8 Time Stamps AU-8(1) Synchronization With Authoritative Sources	Implemented Network Time Protocol by using Chronyd service.
AU-9 Protection of Audit Information AU-9(4) Access By Subset of Privileged users AU-12(3) Changes By Authorized Individual	Implemented ACL on the audit config files so that only root or users with root privileges can write. Applied sticky bit on the Audit logs so that users without root privileges cannot delete them.
AU-11 Audit Record Retention	Configured Auditd to retain logs for a week before they are rotated.
CA-3 System Interconnection CA-3(2) Classified National Security System Connections CA-3(5) Restriction on External Network Connections	Configured the firewall to deny all connections by by default and accept connections from only the known ip addresses by adding rich rules.
CM-7 Least Functionality	All unused ports and services was turned off.
CM-11(2) User Installed Software | Prohibit Installation Without Privileged Status	Command used to install software such as the yum tool was make to work only for users with root privileges.

CP-2(3) Contingency Plan | Resume Essential Mission Functions CP-10 Information System Recovery and Reconstruction	The operating system runs on a virtual machine, in case of any contingency a stable snapshot of the OS configuration can be loaded for use.
IA-2 Identification And Authentication	implemented public key authentication with ssh.
IA-2(1) Network Access To privileged Accounts	implemented public key authentication along with password for privileged accounts over ssh.
IA-2(2) Network Access to Non privileged Accounts	implemented public key authentication along with password for non privileged accounts over ssh.
IA-3 Device Identification and Authentication	Devices are uniquely identified by configuring firewall and public key authentication.
IA-4 Identifier Management	Users are identified by their user name and UID
IA-5 Authenticator Management	Password and PKI certificates set for the users.
IA-5(1) Password Based Authentication	Passwords were set for users.
IA-5(2) PKI Based Authentication SC-17 Public Key Infrastructure Certificates	Public and private keys were generated and ssh was configured for public key authentication.
IA-5(4) Automated Support For Password Strength Determination	The operating system inherently prompts level of password strength when a password is being set.
IA-5(7) No Embedded Unencrypted Static Authenticators	Users passwords are stored in hashed forms in /etc/shadows file.
MA-4 Nonlocal Maintenance MA-4(6) Cryptographic Protection	Ssh server has been implemented for SysAdmins to remotely login by using a ssh client. Ssh was configured to use public key authentication.
PE-10 Emergency Shut Off	A physical button has been put on the robot to power it off. It can also be triggered remotely.
PE-14 Temperature and Humidity Control	A fan has been installed inside the robot.
SC-5 Denial Of Service Protection	Installed DDOS Deflate which is a lightweight bash shell script designed to assist in the process of blocking a denial of service attack. It create a list of IP addresses connected to the server, along with their total number of connections.

SC-7 Boundary Protection	Configured firewalld service.
SC-7(5) Deny by Default/ Allow By Exception	Configured the firewall to allow connection of specific services and ports from specific devices.
SC-7(11) Restrict Incoming Communicational Traffic	Firewall has been configured to allow only known ip to connect.
SC-7(12) Host Based Protection	The firewall implemented is host based
SC-8 Transmission Confidentiality and Integrity SC-8(1) Cryptographic or Alternate Physical	Communication is encrypted over ssh.
SI-3 Malicious Code Protection	installed CalmAV.
SI-4 Information System Monitoring	installed and configured monit to monitor the system through a web portal.

C. Description of appropriate but unimplemented controls

ID	***Description***
AC-2(4)	Account Management | Automated Audit Actions
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts
AC-2(10)	Account Management | Shared / Group Account Credential Termination
AC-10	Concurrent Session Control
AC-14	Permitted Actions Without Identification or Authentication
AC-17(4)	Remote Access | Privileged Commands / Access
AC-18(5)	Wireless Access | Antennas / Transmission Power Levels
AC-21	Information Sharing
AT-1	Security Awareness
AT-3	Role-Based Security Training
AT-3(4)	Security Training | Suspicious Communications & Anomolous System Behaviour
AT-4	Security Training Records
AU-1	Audit & Accountability Policy And Procedures
AU-2	Audit Events
AU-2(3)	Audit Events | Reviews And Updates
AU-3(1)	Content of Audit Records | Additional Audit Information
AU-3(2)	Content of Audit Records | Centralized Management of Planned Audit Record Content

AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-5(1)	Response to Audit Processing Failures | Audit Storage Capacity
AU-5(2)	Response to Audit Processing Failures | Real-TIme Alerts
AU-6	Audit Review, Analysis And Reporting
AU-7	Audit Reduction and Report Generation
AU-7(1)	Audit Reduction and Report Generation | Automatic Processing
AU-9(2)	Protection of Audit Information | Audit Backup on separate Physical Systems / Components
AU-9(3)	Protection of Audit Information | Cryptographic Protection
AU-10	Non-Repudiation
AU-11(1)	Audit Record Retention | Long-Term Retrieval Capability
CA-1	Security Assessment And Authorization Policies And Procedures
CA-2	Security Assessments
CA-2(1)	Security Assessments | Independent Accessors
CA-2(2)	Security Assessments | Specialized Assessments
CA-5	Plan of Action and Milestones
CA-6	Security Authorization
CA-7	Continuous Monitoring
CA-8	Penetration Testing
CM-1	Configuration Management Policy And Procedures
CM-2(1)	Baseline Configuration | Reviews And Updates
CM-2(2)	Baseline Configuration | Automation Support for Accuracy / Currency
CM-2(7)	Baseline Configuration | Configure Systems, Components or Devices for High-Risk Areas
CM-3	Configuration Change Control
CM-3(1)	Configuration Change Control | Automated Document / Notification / Prohibition of Changes
CM-3(2)	Configuration Change Control | Test / Validate / Document Changes
CM-3(5)	Configuration Change Control | Automated Security Response
CM-3(6)	Configuration Change Control | Cryptography Management
CM-4	Security Impact Analysis

CM-4(1)	Security Impact Analysis | Separate Test Environments
CM-5	Access Restrictions For Change
CM-5(1)	Access Restrictions For Change | Automated Access Enforcement / Auditing
CM-5(2)	Access Restrictions For Change | Review System Changes
CM-5(3)	Access Restrictions For Change | Signed Components
CM-6	Configuration Settings
CM-6(1)	Configuration Settings | Automated Central Management / Application / Verification
CM-6(2)	Configuration Settings | Respond to Unauthorized Changes
CM-7(1)	Least Functionality | Periodic Review
CM-7(2)	Least Functionality | Prevent Program Execution
CM-8(1)	Information System Component Inventory | Updates During Installations / Removals
CM-8(2)	Information System Component Inventory | Automated Maintenance
CM-8(3)	Information System Component Inventory | Automated Unauthorized Component Detection
CM-8(4)	Information System Component Inventory | Accountability Information
CM-8(5)	Information System Component Inventory | No Duplicate Accounting of Components
CM-9	Configuration Management Plan
CM-11(1)	User-Installed Software | Alerts For Unauthorized Installations
CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-2(1)	Contingency Plan | Coordinate With Related Plans
CP-2(2)	Contingency Plan | Capacity Planning
CP-2(4)	Contingency Plan | Resume All Missions / Business Functions
CP-2(5)	Contingency Plan | Continue Essential Missions / Business Functions
CP-2(8)	Contingency Plan | Identify Critical Assets
CP-3	Contingency Training
CP-3(1)	Contingency Training | Simulated Events
CP-4	Contingency Plan Testing
CP-4(1)	Contingency Plan Testing | Coordinate With Related Plans
CP-8	Telecommunications Services

CP-8(1)	Telecommunications Services | Priority of Service Provisions
CP-8(2)	Telecommunications Services | Single Points of Failure
CP-8(3)	Telecommunications Services | Separation of Primary / Alternate Providers
CP-8(4)	Telecommunications Services | Provider Contingency Plan
CP-9	Information System Backup
CP-9(1)	Information System Backup | Testing For Reliability / Integrity
CP-9(3)	Information System Backup | Separate Storage for Critical Information
CP-10(4)	Information System Recovery and Reconstitution | Restore Within Time Period
IA-1	Identification and Authentication Policy and Procedures
IA-2(3)	Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts
IA-2(4)	Identification and Authentication (Organizational Users) | Local Access to Non-Privileged Accounts
IA-2(8)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Replay Resistant
IA-2(9)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts - Replay Resistant
IA-2(11)	Identification and Authentication (Organizational Users) | Remote Access - Separate Device
IA-2(12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials
IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication
IA-5(3)	Authenticator Management | In Person or Trusted Third-Party Registration
IA-5(8)	Authenticator Management | Multiple Information System Accounts
IA-5(11)	Authenticator Management | Hardware Token-Based Authentication
IA-5(14)	Authenticator Management | Managing Content of PKI Trust stores
IA-7	Cryptographic Module Authentication
IA-8	Identification and Authentication (Non-Organizational Users)
IA-8(1)	Identification and Authentication (Non-Organizational Users) | Acceptance of PIV Credentials from Other Agencies
IA-11	Re-authentication
IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training

IR-2(1)	Incident Response Training | Simulated Events
IR-2(2)	Incident Response Training | Automated Training Environments
IR-3	Incident Response Testing
IR-3(2)	Incident Response Testing | Coordination With Related Plans
IR-4(1)	Incident Handling | Automated Incident Handling Processes
IR-4(4)	Incident Handling | Information Correlation
IR-4(6)	Incident Handling | Insider Threats - Specific Capabilities
IR-4(7)	Incident Handling | Insider Threats - Intra-Organization Coordination
IR-4(8)	Incident Handling | Correlation With External Organizations
IR-5(1)	Incident Monitoring | Automated Tracking / Data Collection / Analysis
IR-6(1)	Incident Reporting | Automated Reporting
IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents
IR-7	Incident Response Assistance
IR-7(1)	Incident Response Assistance | Automation Support For Availability of Information / Support
IR-7(2)	Incident Response Assistance | Coordination With External Providers
IR-8	Incident Response Plan
MA-1	System Maintenance Policy and Procedures
MA-2	Controlled Maintenance
MA-2(2)	Controlled Maintenance | Automated Maintenance Activities
MA-3	Maintenance Tools
MA-3(1)	Maintenance Tools | Inspect Tools
MA-3(2)	Maintenance Tools | Inspect Media
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal
MA-4(1)	Nonlocal Maintenance | Auditing and Review
MA-4(2)	Nonlocal Maintenance | Document Nonlocal Maintenance
MA-4(7)	Nonlocal Maintenance | Remote Disconnect Verification
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
MP-1	Media Protection Policy and Procedures
MP-2	Media Access
MP-6	Media Sanitization

PE-1	Physical and Environmental Protection Policy and Procedures
PE-2	Physical Access Authorizations
PE-3	Physical Access Control
PE-3(1)	Physical Access Control | Information System Access
PE-6	Monitoring Physical Access
PE-6(4)	Monitoring Physical Access | Monitoring Physical Access to Information Systems
PE-11	Emergency Power
PE-11(1)	Emergency Power | Long-Term Alternate Power Supply - Minimal Operational Capability
PL-1	Security Planning Policy and Procedures
PL-4	Rules of Behavior
PS-2	Position Risk Designation
PS-3	Personnel Screening
SA-3	System Development Life Cycle
SA-4(9)	Acquisition Process | Functions / Ports / Protocols / Services in Use
SA-4(10)	Acquisition Process | Use of Approved PIV Products
SA-5	Information System Documentation
SA-8	Security Engineering Principles
SA-9	External Information System Services
SC-5(3)	Denial of Service Protection | Detection / Monitoring
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers
SC-7(9)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic
SC-7(21)	Boundary Protection | Isolation of Information System Components
SC-15	Collaborative Computing Devices
SC-18	Mobile Code
SC-18(4)	Mobile Code | Prevent Automatic Execution
SI-1	System and Information Integrity Policy and Procedures
SI-2(5)	Flaw Remediation | Automatic software / Firmware Updates
SI-2(6)	Flaw Remediation | Removal of Previous Versions of Software / Firmware
SI-4(2)	Information System Monitoring | Automated Tools For Real-Time Analysis
SI-4(20)	Information System Monitoring | Privileged User
SI-7	Software, Firmware, and Information Integrity

SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks
SI-7(5)	Software, Firmware, and Information Integrity | Automated Response to Integrity Violations
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response
SI-7(8)	Software, Firmware, and Information Integrity | Auditing Capability For Significant Events
SI-12	Information Handling and Retention
SI-16	Memory Protection

Description of cyber control demonstration strategy

Controls	***Demonstration Strategy***
AC-2 Account management AC-3 Access Enforcement AC-17 Remote Access IA-2 Identification And Authentication IA-2(1) Network Access To privileged Accounts IA-2(2) Network Access to Non privileged Accounts IA-5 Authenticator Management IA-5(1) Password Based Authentication MA-4 Nonlocal Maintenance	Will Login to a non privileged user account and the root account with the right credentials from the host system running on a virtual machine.
AC-2(2) Removal of temporary / Emergency accounts	Will run a script in the host system which creates a temporary account for 30 seconds. Will login to the temporary user account and re login in 30 seconds to show that the user no longer exists.
AC-2(5) Inactivity Logout AC-12 Session Termination	Will login to a user and show that the user gets automatically logged out after 30 seconds of inactivity.
AC-2(7) Role-based Schemes	Will log in to different user accounts with and without privileges and demonstrate the output of trying to edit files like /etc/hosts while need administrative privileges.

AC-2(13) Disable Accounts for High-Risk Individual	Will run a command to disable the root account then will try to login to root to demonstrate that it fails.
AC-4 Information Flow Enforcement AC-17 Remote Access AC-17(2) Protection of Confidentiality/ Integrity Using Encryption AC-19 Access Control For Mobile Device CA-3(2) Classified National Security System Connections CA-3(5) Restriction on External Network Connections IA-3 Device Identification and Authentication IA-5(2) PKI Based Authentication SC-17 Public Key Infrastructure Certificates MA-4(6) Cryptographic Protection SC-7 Boundary Protection SC-7(5) Deny by Default/ Allow By Exception SC-7(12) Host Based Protection SC-7(11) Restrict Incoming Communicational Traffic	Will try to make remote login connection using ssh from 2 different virtual systems to the host. The remote login would be for the same user. Connection from one of the virtual system would succeed and the other would fail demonstrating whitelisting in firewall of the host system. Will demonstrate the use of public key authentication by logging in to the user without using the user's password but a private key and a pass phrase.
AC-5 Separation of Duty AC-6 Least Privilege	Will try to access the same directory from two different user accounts belonging to different groups and demonstrate that only one will be able access it.
AC-6(1) Authorize Access To Security Functions AC-6(10) Prohibit Non Privileged Users from Executing Privileged Functions	Will execute a security functions like starting a starting a service from a privileged and a non privileged user to demonstrate that only the privileged user can carry out the function.
AC-6(2) Non-Privileged Access For Nonsecurity Functions	Will execute a non security function like listing all run-in processes from both privileged and non privileged users.
AC-6(8) Privilege Level For Code Execution AC-6(9) Auditing The Use Of Privileged Functions	Will list all the executable files which is owned by root and has SUID(privilege escalation) set on it by the use of "find" command and lynis tool. This will demonstrate that no such executable code exists.
AC-8 System Use Notification	Will remote login to the host to display the system use message.

AC-11 Session Lock	Will demonstrate that after 30 seconds of inactively the host machine locks out the user.
AC-11(1) Pattern-Hiding Display	Will demonstrate that the desktop background and all the opened files gets hidden under a lock screen.
AC-12(1) User-initiated Logouts/ Message Displays	Will demonstrate that on logout a message is displayed on the screen of the terminal.
AC-17(1) Automated Monitoring SI-4 Information System Monitering	Will open a website which is being hosted by the robot system which contains informations about the services being monitored. Will shutdown the sshd service in the robot system which will be notified in the website as well as through email to the system administrator.
AC-17(9) Disconnect / Disable Access	Will try to remotely login for a user and will also try to login to the same user account from the robot system and demonstrate that the remote login doesn’t work but logging in locally works.
AC-19 Access Control For Mobile Device CM-7 Least Functionality	Will list all the open ports and services to show that there are no unnecessary ports and services running.
AU-3 Content of Audit Record AU-12 Audit generation	Will open and show the audit logs of the system.
AU-8 Time Stamps AU-8(1) Synchronization With Authoritative Sources	Will show that the time is synchronised between the robot system and another system.
AU-9 Protection of Audit Information AU-9(4) Access By Subset of Privileged users AU-12(3) Changes By Authorized Individual	Will try to delete audit records from a non privileged user account and show that it is unsuccessful in doing so.
AU-11 Audit Record Retention	Will list the total files of the audit logs.
CM-11(2) User Installed Software | Prohibit Installation Without Privileged Status	Will execute the yum command to download a package from a non privileged account to demands that it needs admin privileges to execute.

CP-2(3) Contingency Plan | Resume Essential Mission Functions CP-10 Information System Recovery and Reconstruction	Will delete crucial file from a privileged user account and then load back the configured operating system from an earlier snapshot of the virtual machine.
IA-4 Identifier Management	Will display the usernames and UIDs stored in the system.
IA-5(7) No Embedded Unencrypted Static Authenticators	Will open the /etc/shadows file to show that the password are not stored In plain text.
PE-10 Emergency Shut Off	Will demonstrate that the robot powers off wren the emergency button is pressed.
PE-14 Temperature and Humidity Control	Will show the working of the fan installed in the robot.
SI-3 Malicious Code Protection	will try to install a malicious code which would trigger the calmAV tool.