Assignment 3 - CCI and Incident Response
CCI Assessment Guide
CSE 4380

Group Thorin

April 11th, 2025

Members:	Obadah Al-Smadi
	Betim Hodza
	Elliot Mai
	Benjamin Niccum
	Nicholas Pratt
Instructor:	Trevor Bakker

Contents

List of Figures

List of Tables

1 Assessment Methodology

1.1 Overall Approach

The assessment of Control Correlation Identifiers (CCIs) for the X9 UAV system follows a structured methodology aligned with NIST SP 800-53A Revision 5. This approach ensures a comprehensive evaluation of security controls implemented within the system. The process includes the following steps:

1. **Planning**: Define the assessment scope, identify applicable CCIs based on the X9 UAV system's security categorization, and develop detailed assessment plans outlining objectives and resources.

2. **Evidence Collection**: Gather relevant documentation (e.g., policies, logs), conduct interviews with system administrators and stakeholders, and perform technical testing to obtain evidence of control implementation.

3. **Analysis**: Evaluate collected evidence against predefined compliance criteria to assess the effectiveness and completeness of each control.

4. **Reporting**: Document assessment findings, highlight any deficiencies, and provide actionable recommendations for remediation to ensure compliance with NIST standards.

The assessment will be conducted by a team of qualified security assessors with expertise in unmanned aerial vehicle (UAV) systems and NIST security frameworks, ensuring a thorough and accurate evaluation.

1.2 Evidence Collection Standards

Evidence collection for the X9 UAV system CCI assessment adheres to the following standards to ensure consistency, reliability, and traceability:

- **Documentation Review**: All reviewed documents (e.g., System Security Plan, configuration files) must be current, officially approved by authorized personnel, and directly relevant to the assessed controls.

- **Interviews**: Conduct structured interviews with key personnel responsible for implementing and managing security controls. Responses will be documented in detail and cross-verified with other evidence sources (e.g., logs, test results).

- **Technical Testing**: Perform testing in controlled environments using approved tools and methodologies. Test results will be systematically logged, timestamped, and analyzed for compliance with CCI requirements.

- **Sampling**: Where applicable, employ statistical sampling techniques (e.g., 95% confidence level) to select representative samples of accounts, logs, or transactions for assessment, ensuring scalability and efficiency.

These standards ensure that evidence is robust, verifiable, and sufficient to support compliance determinations.

2 Assessment Procedures by Control Family

2.1 Access Control (AC) CCIs

2.1.1 CCI-000213: Account Management

Assessment Procedures Review the X9 UAV user and admin account configurations to verify implementation of account management controls. Inspect account creation, modification, and termination logs. Interview system administrators to confirm understanding of account management procedures. Simulate account lifecycle events (creation, modification, deactivation) and validate workflow execution.

Evidence Requirements

- Account management policy documentation with approval signatures.
- Access control lists showing user privileges.
- Account activity logs with timestamps and action details.
- Screenshots of account management interfaces.
- Administrator training records on account management protocols.

Testing Methodology Perform functional testing by creating test accounts and verifying privilege assignments. Execute automated scripts to validate account inactivity timeouts. Conduct penetration tests attempting to bypass account management controls.

Compliance Criteria

- Account creation requires documented approval from authorized personnel.
- Inactive accounts are disabled after 30 days of inactivity.
- 100% of account terminations are processed within 24 hours of request.
- Separation of duties is enforced for privileged account management.

Evaluation Methods Compare account management controls against NIST SP 800-53 R5 requirements. Analyze account activity logs for timeliness and completeness. Conduct statistical sampling of account records to verify compliance (95

2.2 Audit and Accountability (AU) CCIs

Since the X9's current Control Traceability Matrix concludes that the organization handles it, there are no implementations here per NIST SP 800-53 Revision 5. If system-level responsibilities are assigned in the future, assessments can be developed based on CCI List and NIST SP 800-161 Rev. 1

2.3 Assessment Authorization and Monitoring (CA) CCIs

Since the X9's current Control Traceability Matrix concludes that the organization handles it, there are no implementations here per NIST SP 800-53 Revision 5. If system-level responsibilities are assigned in the future, assessments can be developed based on CCI List and NIST SP 800-161 Rev. 1

2.4 Configuration Management (CM) CCIs

Evidence Requirements

- Change approval workflow configurations.
- Logs of approval attempts, including unauthorized ones.
- Test results from simulated unauthorized approvals.
- Training records for change control administrators.

Testing Methodology Deploy test changes to validate approval workflows. Simulate unauthorized approval attempts to ensure rejection. Use automated tools to verify approval enforcement. Monitor logs for approval activities.

Compliance Criteria

- 100% of changes require authorized approval.
- Unauthorized approval attempts are blocked within 10 seconds.
- Approval logs are retained for at least 90 days.

Evaluation Methods Analyze approval workflow configurations against policy requirements. Review logs to confirm unauthorized approval detection. Conduct scenario-based interviews with administrators. Use testing tools to validate approval enforcement.

2.4.1 CCI-003942: Configuration Change Control

Assessment Procedures Review the change control process for the X9 and GCS to ensure change implementation is tracked. Inspect implementation logs for timestamps and executor details. Simulate a change to test tracking accuracy. Interview change managers to confirm tracking processes.

Evidence Requirements

- Change implementation logs with timestamps and executor details.
- Change control policy documents.
- Test results from simulated changes.
- Training records for change managers.

Testing Methodology Deploy test changes to validate implementation tracking. Use automated tools to verify log accuracy. Simulate untracked changes to test detection. Monitor logs for implementation tracking events.

Compliance Criteria

- 100% of changes are tracked with timestamps and executor details.
- Untracked changes are detected within 10 seconds.
- Implementation logs are retained for at least 90 days.

Evaluation Methods Analyze implementation logs against policy requirements. Review test results to confirm tracking accuracy. Conduct scenario-based interviews with change managers. Use testing tools to validate tracking integrity.

2.4.2 CCI-000366: Configure System for Least Functionality

Assessment Procedures Review the X9 and GCS configurations to ensure only essential functions are enabled. Inspect system service lists to verify non-essential services are disabled. Simulate enabling a non-essential service to test detection. Interview system administrators to confirm least functionality practices.

Evidence Requirements

- System configuration files showing disabled non-essential services.
- Logs of service enablement attempts.
- Test results from simulated non-essential service enablement.
- Training records for system administrators.

Testing Methodology Deploy test configurations to validate least functionality settings. Simulate enabling non-essential services to ensure detection. Use automated tools to verify service restrictions. Monitor logs for service management activities.

Compliance Criteria

- 100% of non-essential services are disabled.
- Unauthorized service enablement is detected within 10 seconds.
- Service configuration logs are retained for at least 30 days.

Evaluation Methods Compare system configurations against least functionality policies. Analyze logs to confirm unauthorized service detection. Conduct scenario-based interviews with administrators. Use testing tools to validate service restrictions.

2.4.3 CCI-003943: Software Usage Restrictions

Assessment Procedures Review processes for monitoring software usage on the X9 and GCS to ensure compliance with restrictions. Inspect usage monitoring tools and logs. Simulate unauthorized software usage to test monitoring effectiveness. Interview monitoring personnel to confirm processes.

Evidence Requirements

- Software usage monitoring tool configurations.
- Logs of software usage monitoring events.
- Test results from simulated unauthorized usage.
- Training records for monitoring personnel.

Testing Methodology Deploy test software to validate monitoring tool effectiveness. Simulate unauthorized software usage to ensure detection. Use automated tools to verify monitoring coverage. Monitor logs for usage monitoring events.

Compliance Criteria

- 100% of software usage is monitored.
- Unauthorized usage is detected within 10 seconds.
- Monitoring logs are retained for at least 30 days.

Evaluation Methods Analyze monitoring tool configurations against policy requirements. Review logs to confirm unauthorized usage detection. Conduct scenario-based interviews with monitoring personnel. Use testing tools to validate monitoring effectiveness.

2.4.4 CCI-003944: Software Usage Restrictions

Assessment Procedures Inspect enforcement mechanisms for software usage restrictions on the X9 and GCS. Verify that unauthorized software is blocked from execution. Simulate executing unauthorized software to test enforcement. Interview security administrators to confirm enforcement processes.

Evidence Requirements

- Configuration files for software execution restrictions.
- Logs of software execution attempts.
- Test results from simulated unauthorized executions.
- Training records for security administrators.

Testing Methodology Deploy test software to validate execution restrictions. Simulate unauthorized software execution to ensure blocking. Use automated tools to verify execution controls. Monitor logs for execution restriction activities.

Compliance Criteria

- 100% of unauthorized software is blocked from execution.
- Unauthorized execution attempts are detected within 10 seconds.
- Execution restriction logs are retained for at least 30 days.

Evaluation Methods Analyze execution restriction configurations against policy requirements. Review logs to confirm unauthorized execution detection. Conduct scenario-based interviews with security administrators. Use testing tools to validate execution controls.

2.4.5 CCI-003945: User-installed Software

Assessment Procedures Review policies for user-installed software on the X9 and GCS to ensure restrictions are enforced. Inspect system configurations to block unauthorized installations. Simulate a user attempting to install software to test enforcement. Interview system administrators to confirm restriction processes.

Evidence Requirements

- User-installed software policy documents.
- System configuration files for installation restrictions.
- Logs of installation attempts by users.
- Training records for system administrators.

Testing Methodology Deploy test user accounts to validate installation restrictions. Simulate unauthorized software installations to ensure blocking. Use automated tools to verify installation controls. Monitor logs for installation restriction activities.

Compliance Criteria

- 100% of user-installed software is blocked unless authorized.
- Unauthorized installation attempts are detected within 10 seconds.
- Installation restriction logs are retained for at least 30 days.

Evaluation Methods Analyze installation restriction configurations against policy requirements. Review logs to confirm unauthorized installation detection. Conduct scenario-based interviews with administrators. Use testing tools to validate installation controls.

2.4.6 CCI-003946: User-installed Software

Assessment Procedures Inspect monitoring mechanisms for user-installed software on the X9 and GCS. Verify that unauthorized installations trigger alerts. Simulate an unauthorized installation to test monitoring effectiveness. Interview security analysts to confirm monitoring processes.

Evidence Requirements

- Monitoring tool configurations for user-installed software.
- Logs of unauthorized installation alerts.
- Test results from simulated unauthorized installations.
- Training records for security analysts.

Testing Methodology Deploy test user accounts to simulate unauthorized installations. Use monitoring tools to validate alert generation. Conduct tests to ensure comprehensive monitoring coverage. Monitor logs for installation monitoring events.

Compliance Criteria

- 100% of unauthorized installations trigger alerts within 10 seconds.
- Monitoring covers all system components.
- Monitoring logs are retained for at least 30 days.

Evaluation Methods Analyze monitoring configurations against policy requirements. Review logs to confirm unauthorized installation alerts. Conduct scenario-based interviews with security analysts. Use testing tools to validate monitoring effectiveness.

2.4.7 CCI-000381: Configure System to Avoid Unnecessary Functions

Assessment Procedures Review the X9 and GCS configurations to ensure unnecessary functions are disabled. Inspect system configurations for disabled non-critical features. Simulate enabling an unnecessary function to test detection. Interview system administrators to confirm configuration practices.

Evidence Requirements

- Configuration files showing disabled unnecessary functions.
- Logs of function enablement attempts.
- Test results from simulated unnecessary function enablement.
- Training records for system administrators.

Testing Methodology Deploy test configurations to validate function restrictions. Simulate enabling unnecessary functions to ensure detection. Use automated tools to verify function controls. Monitor logs for function management activities.

Compliance Criteria

- 100% of unnecessary functions are disabled.
- Unauthorized function enablement is detected within 10 seconds.
- Function configuration logs are retained for at least 30 days.

Evaluation Methods Analyze configuration files against least functionality policies. Review logs to confirm unauthorized function detection. Conduct scenario-based interviews with administrators. Use testing tools to validate function restrictions.

2.4.8 CCI-003948: Configure System to Avoid Unnecessary Functions

Assessment Procedures Inspect the X9 and GCS to ensure only mission-critical functions are enabled. Verify that non-critical functions are documented and disabled. Simulate enabling a non-critical function to test enforcement. Interview system administrators to confirm function management processes.

Evidence Requirements

- Documentation of mission-critical functions.
- Configuration files for disabled non-critical functions.
- Logs of function enablement attempts.
- Training records for system administrators.

Testing Methodology Deploy test configurations to validate critical function enforcement. Simulate non-critical function enablement to ensure detection. Use automated tools to verify function restrictions. Monitor logs for function management activities.

Compliance Criteria

- 100% of non-critical functions are disabled.
- Unauthorized function enablement is detected within 10 seconds.
- Function management logs are retained for at least 30 days.

Evaluation Methods Compare function configurations against mission-critical requirements. Analyze logs to confirm non-critical function detection. Conduct scenario-based interviews with administrators. Use testing tools to validate function restrictions.

2.5 Contingency Planning (CP) CCIs

Since the X9's current Control Traceability Matrix concludes that the organization handles it, there are no implementations here per NIST SP 800-53 Revision 5. If system-level responsibilities are assigned in the future, assessments can be developed based on CCI List and NIST SP 800-161 Rev. 1

2.6 Identification and Authentication (IA) CCIs

2.6.1 CCI-000764: Unique User Identification

Assessment Procedures Review user account configurations for the X9 drone and GCS to ensure each user has a unique identifier. Inspect account databases for duplicate IDs. Simulate a login attempt with a non-unique ID to test system response. Interview system administrators to confirm ID assignment processes.

Evidence Requirements

- User account database excerpts showing unique IDs.
- Logs from simulated non-unique ID login attempts.
- Account management policy documents.
- Training records for system administrators.

Testing Methodology Deploy test accounts to validate unique ID enforcement. Attempt to create duplicate IDs to ensure rejection. Use automated tools to scan account databases for duplicates. Monitor logs for account creation and login events.

Compliance Criteria

- 100% of users have unique identifiers.
- Non-unique ID creation attempts are blocked within 1 second.
- Account logs are retained for at least 90 days.

Evaluation Methods Analyze account configurations against policy requirements. Review logs to confirm duplicate ID rejection. Conduct scenario-based interviews with administrators. Use testing tools to validate unique ID enforcement.

2.6.2 CCI-001941: Authenticator Management

Assessment Procedures Inspect authenticator management policies for the X9 and GCS to ensure secure password issuance. Verify that initial authenticators meet complexity requirements (e.g., 12 characters, mixed case). Simulate an authenticator issuance to test compliance. Interview security administrators to confirm management processes.

Evidence Requirements

- Authenticator policy documents specifying complexity.
- Logs of authenticator issuance events.
- Test results from simulated issuance scenarios.
- Training records for security administrators.

Testing Methodology Deploy test accounts to validate authenticator complexity enforcement. Simulate weak authenticator issuance to ensure rejection. Use automated tools to verify password strength. Monitor logs for authenticator management activities.

Compliance Criteria

- 100% of authenticators meet complexity requirements.
- Weak authenticator issuance is blocked within 1 second.
- Authenticator logs are retained for at least 90 days.

Evaluation Methods Compare authenticator policies against security standards. Analyze logs to confirm complexity enforcement. Conduct scenario-based interviews with administrators. Use testing tools to validate authenticator management.

2.7 Incendent Response (IR) CCIs

2.7.1 CCI-000831: Capability to Automatically Disable the System

Assessment Procedures Review X9 UAV and GCS configuration settings to verify detection of defined security violations (e.g., unauthorized access attempts, tampered firmware). Afterwards, inspect shutdown trigger configurations (e.g., 3 failed authentication attempts) in system software. Then simulate security violations in a test environment to trigger automatic disabling. Analyze shutdown logs for accuracy and completeness of recorded events. Interview incident response team to confirm understanding of shutdown procedures.

Evidence Requirements
The Evidence we need follows:

- Configuration files showing security violation detection settings.
- Logs of simulated shutdown events with timestamps, violation types, and system states.
- Test reports from controlled environment testing.
- Documentation of shutdown triggers in the X9 IR Plan.
- Training records for incident response team on shutdown protocols.

Testing Methodology We will perform functional testing by simulating 3 failed authentication attempts and verifying system shutdown. Then conduct penetration tests to inject malicious code and confirm automatic disabling. Afterwards we will validate log integrity using checksums or cryptographic signatures.

To make this more streamlined we will use automated scripts to repeat tests across multiple scenarios (e.g., GCS standalone, UAV in flight).

Compliance Criteria

- System disables within 5 seconds of detecting a defined security violation.
- 100% of shutdown events are logged with required details (timestamp, violation type, system state).
- All simulated tests result in successful automatic disabling without manual intervention.
- Incident response team demonstrates procedural knowledge in interviews.

Evaluation Methods We will compare test results against compliance criteria in NIST-800-53 R5 using pass or fail metrics. Then we will analyze log data based on completeness with statistical sampling (e.g. 95% confidence level). We'll check back once again on the assessor for their observations from the simulations to see if they all come back consistent, and finally we will do a compliance review meeting with X9's security team to validate what we have found.

2.8 Media Protection (MP) CCIs

Since the X9's current Control Traceability Matrix concludes that the organization handles it, there are no implementations here per NIST SP 800-53 Revision 5. If system-level responsibilities are assigned in the future, assessments can be developed based on CCI List and NIST SP 800-161 Rev. 1

2.9 Physical and Environmental Protection (PE) CCIs

Since the X9's current Control Traceability Matrix concludes that the organization handles it, there are no implementations here per NIST SP 800-53 Revision 5. If system-level responsibilities are assigned in the future, assessments can be developed based on CCI List and NIST Cybersecurity Framework.

2.10 Planning (PL) CCIs

2.10.1 CCI-001234: System Security Plan Development

Assessment Procedures Review the X9 UAV System Security Plan (SSP) to verify inclusion of system boundaries, security controls, and implementation details. Inspect version control logs for SSP updates. Interview stakeholders to confirm coordination during plan development. Simulate a system change (e.g., new telemetry module) and validate SSP update workflows.

Evidence Requirements

- Finalized SSP document with approval signatures.
- Version control logs showing SSP updates.
- Meeting minutes from stakeholder coordination sessions.
- Test records demonstrating SSP update workflows.

Testing Methodology Conduct functional testing by modifying system components and verifying SSP updates. Use automated scripts to validate version control enforcement. Perform tabletop exercises with stakeholders to test coordination processes.

Compliance Criteria

- SSP includes all NIST SP 800-53 R5-required elements.
- SSP updates occur within 5 business days of system changes.
- 100% of stakeholders confirm awareness of SSP roles.

Evaluation Methods Compare SSP against NIST SP 800-53 R5 Appendix H checklist. Analyze version control logs for timeliness. Conduct statistical sampling of stakeholder interviews (95% confidence level).

2.11 Program Management (PM) CCIs

2.11.1 CCI-002567: Centralized Program Governance

Assessment Procedures Inspect PM dashboards for real-time metrics (e.g., vulnerability remediation rates). Review role assignments for program leadership. Simulate a compliance violation and verify escalation workflows. Interview PMO staff to confirm understanding of governance processes.

Evidence Requirements

- Screenshots of PM dashboards showing security metrics.
- Role assignment documents with approval signatures.
- Escalation workflow diagrams and test records.
- PMO training records on governance protocols.

Testing Methodology Inject simulated compliance gaps (e.g., overdue patches) and validate dashboard alerts. Conduct penetration tests on PM tools to ensure secure access. Perform role-based access control (RBAC) validation for PM dashboards.

Compliance Criteria

- Dashboards reflect metrics with ¡=1-hour latency.
- 100% of compliance violations trigger alerts within 15 minutes.
- RBAC configurations align with separation of duties requirements.

Evaluation Methods Compare dashboard data against ground truth sources. Analyze alert timestamps using automated scripts. Conduct compliance reviews with PMO leadership.

2.12 Risk Assessment (RA) CCIs

2.12.1 CCI-003891: Vulnerability Scanning

Assessment Procedures Review vulnerability scanner configurations for coverage of drone components (flight software, GCS). Inspect scan schedules and historical records. Simulate a critical vulnerability and validate prioritization in remediation workflows. Interview security analysts to confirm scan result handling.

Evidence Requirements

- Scanner configuration files showing asset coverage.
- Scan reports with timestamps and vulnerability details.
- Remediation tickets from simulated critical vulnerabilities.
- Analyst training records on scan tools.

Testing Methodology Deploy test vulnerabilities (e.g., outdated libraries) and validate scanner detection. Conduct unauthenticated scans to simulate attacker reconnaissance. Use automated scripts to validate scan frequency adherence.

Compliance Criteria

- 100% of critical vulnerabilities detected within 24 hours.
- Scanner coverage includes all API endpoints and firmware.
- Remediation workflows initiate within 2 hours of critical findings.

Evaluation Methods Compare scan results against known vulnerabilities using NVD data. Analyze remediation ticket timestamps. Conduct interviews with analysts using scenario-based questions.

2.13 System and Services Acquisition (SA) CCIs

Since the X9's current Control Traceability Matrix concludes that the organization handles it, there are no implementations here per NIST SP 800-53 Revision 5. If system-level responsibilities are assigned in the future, assessments can be developed based on CCI List and NIST SP 800-161 Rev. 1

2.14 System and Communication Protection (SC) CCIs

2.14.1 CCI-002385: Denial-of-Service Protection Policy and Procedures

Assessment Procedures Review organizational policies addressing denial-of-service (DoS) protections. Examine implemented controls across network gateways and application layers. Interview network engineers on incident response plans for DoS scenarios.

Evidence Requirements

- DoS protection policy and procedures.
- IDS/IPS configuration and logs showing DoS mitigation.
- DoS attack drill reports or tabletop exercise documentation.
- Firewall and rate-limiting rule sets.

Testing Methodology Simulate a DoS condition using controlled network traffic spikes. Validate system responsiveness and mitigation behaviors. Review firewall logs and response times.

Compliance Criteria

- DoS protections deployed at all public interfaces.
- Automated blocking or throttling of traffic exceeding thresholds.
- Documented escalation paths during attack scenarios.

Evaluation Methods Compare policy documents with real-world configurations. Validate via penetration testing results. Interview stakeholders and review incident logs.

2.14.2 CCI-004866: Boundary Protection - External Interfaces Monitored

Assessment Procedures Inspect network architecture diagrams and identify external interfaces. Verify that monitoring solutions (e.g., IDS/IPS) are deployed at these boundaries.

Evidence Requirements

- Network diagrams showing monitored interfaces.
- IDS/IPS logs for inbound/outbound traffic.
- Configuration files showing monitored protocols/ports.

Testing Methodology Use packet capture tools to confirm traffic visibility at boundaries. Simulate unauthorized connections to test detection capabilities.

Compliance Criteria

- 100% of external interfaces are monitored.
- Alerts generated for suspicious or unauthorized access.

Evaluation Methods Review sensor placements and data retention. Validate response to alert scenarios. Interview SOC analysts.

2.14.3 CCI-004867: Boundary Protection - Enforced Policy on Communications

Assessment Procedures Evaluate firewall and proxy configurations for enforcement of access control policies. Review change control records for boundary rule updates.

Evidence Requirements

- Firewall rule sets.
- Access control policy documents.
- Network change control logs.

Testing Methodology Attempt unauthorized communication across restricted zones. Inspect logs for alerts and block actions.

Compliance Criteria

- Only authorized protocols and addresses permitted.
- No open interfaces without justification.

Evaluation Methods Compare actual configuration against policy. Conduct traffic flow tests and validate effectiveness.

2.14.4 CCI-001097: Transmission Confidentiality and Integrity - Encryption Standards

Assessment Procedures Confirm that all data-in-transit is encrypted using approved algorithms. Inspect endpoint configurations and data flows.

Evidence Requirements

- TLS/SSH configuration files.
- Encryption algorithm documentation.
- Logs showing encrypted communication sessions.

Testing Methodology Use tools like Wireshark to verify encryption in use. Attempt downgrade or man-in-the-middle attack simulations.

Compliance Criteria

- All sensitive transmissions use TLS 1.3 or higher.
- No plaintext transmission of authentication or control data.

Evaluation Methods Conduct protocol and cipher suite scans. Inspect logins and data flow packets.

2.14.5 CCI-004868: Transmission Confidentiality - Policy and Controls

Assessment Procedures Review policy on protecting data in transit. Match against implementation of TLS, VPNs, and secure messaging protocols.

Evidence Requirements

- Transmission security policies.
- VPN configuration documentation.
- Logs of encrypted communication sessions.

Testing Methodology Attempt to transmit unencrypted data between components. Verify encryption enforcement blocks.

Compliance Criteria

- Policy mandates encryption for all external and internal sensitive traffic.
- Endpoints refuse unencrypted connections.

Evaluation Methods Inspect endpoint settings, attempt insecure communications, and check rejection logs.

2.14.6 CCI-002418: Cryptographic Key Management Procedures

Assessment Procedures Review procedures for key generation, distribution, storage, rotation, and destruction. Interview key custodians and examine access logs.

Evidence Requirements

- Cryptographic key management policy.
- Key lifecycle audit logs.
- Hardware Security Module (HSM) or key vault configuration.
- Key custodian training records.

Testing Methodology Inspect current key inventory. Attempt to validate expiry and revocation mechanisms. Test key access restrictions.

Compliance Criteria

- Keys use FIPS-validated cryptographic modules.
- Keys are rotated at least annually or upon compromise.
- Access to keys is logged and restricted by role.

Evaluation Methods Compare policy with technical implementation. Cross-check logs with assigned personnel. Validate encryption operations with test data.

2.14.7 CCI-001157: Attribute Association with Information Exchange

Assessment Procedures Evaluate metadata tagging mechanisms in APIs and messaging services. Review how privacy/security attributes are attached and validated during transmission.

Evidence Requirements

- Attribute schema documentation.
- Application code or middleware configuration showing attribute handling.
- Test data flows with visible attribute tags.

Testing Methodology Transmit test messages with missing or altered attributes and observe rejection/handling. Use packet sniffers and application logs.

Compliance Criteria

- All sensitive data exchanges include relevant classification, origin, or privacy tags.
- Attributes cannot be stripped or altered without detection.

Evaluation Methods Inspect APIs and message brokers. Conduct fuzz testing with malformed metadata.

2.14.8 CCI-002455: Minimization of Functionality on Thin Nodes

Assessment Procedures Review system images used on thin client or embedded nodes. Verify unnecessary services are removed and configuration hardening is applied.

Evidence Requirements

- System build and deployment scripts.
- OS hardening checklists and audit reports.
- Comparison between minimal and full system configurations.

Testing Methodology Scan nodes for open ports, services, and installed packages. Verify presence of only essential applications.

Compliance Criteria

- No non-essential applications or services running.
- OS configured for least privilege and minimal access.

Evaluation Methods Use vulnerability scanners and system auditing tools (e.g., Lynis, OpenSCAP) to validate configuration.

2.14.9 CCI-004901: Information Protection at Rest – Encryption Mechanisms

Assessment Procedures Verify storage encryption settings on servers, databases, and endpoint devices. Confirm alignment with policy.

Evidence Requirements

- Encryption configuration files or screenshots.
- FIPS-validated encryption tool documentation.
- Audit logs showing encryption status checks.

Testing Methodology Attempt access to encrypted volumes from unauthorized user accounts. Validate encryption status using system tools.

Compliance Criteria

- All sensitive data at rest is encrypted with AES-256 or equivalent.
- Encryption keys are securely managed (see CCI-002418).

Evaluation Methods Inspect encryption status reports. Attempt test decryption without access to proper credentials.

2.14.10 CCI-004902: Information Protection at Rest – Policy Enforcement

Assessment Procedures Examine enforcement mechanisms (e.g., scripts, GPOs, mobile device policies) for ensuring encryption compliance.

Evidence Requirements

- Policy enforcement documentation.
- Screenshots or scripts enforcing disk encryption.
- Device compliance reports from MDM or EDR tools.

Testing Methodology Deploy non-compliant devices and observe enforcement triggers. Attempt to disable encryption manually and monitor alerts.

Compliance Criteria

- Non-compliant systems are auto-flagged or quarantined.
- Encryption cannot be disabled without elevated authorization.

Evaluation Methods Test compliance tools in a sandbox. Review enforcement logs and automatic responses.

2.14.11 CCI-001199: Operations Security in Development Lifecycle

Assessment Procedures Check for OPSEC reviews during planning, development, and deployment stages. Interview developers on secure handling of sensitive information.

Evidence Requirements

- OPSEC risk assessments.
- Change request and review documentation.
- Developer training logs on operational security.

Testing Methodology Inspect commit histories for hardcoded secrets. Check build servers and repositories for exposed sensitive data.

Compliance Criteria

- OPSEC review required at every major system change.
- No sensitive information in source control or logs.

Evaluation Methods Perform code audits and interviews. Review configuration and build pipelines.

2.14.12 CCI-002530: Process Isolation

Assessment Procedures Examine containerization, virtualization, or OS-level controls that ensure process separation. Review sandboxing implementations.

Evidence Requirements

- OS kernel configuration (e.g., SELinux, AppArmor).
- Docker/Kubernetes isolation settings.
- Audit reports on inter-process communication.

Testing Methodology Attempt to break out of isolated containers or VMs. Monitor system for unauthorized access between processes.

Compliance Criteria

- All critical processes execute in separate memory spaces.
- Isolation mechanisms log unauthorized access attempts.

Evaluation Methods Use penetration testing tools and system call tracing to validate isolation boundaries.

2.14.13 CCI-002536: Wireless Link Protection

Assessment Procedures Review wireless configurations and encryption policies. Inspect site survey logs and rogue AP detection tools.

Evidence Requirements

- Wireless configuration files.
- WPA3 or 802.1X deployment documentation.
- Logs from wireless intrusion detection systems.

Testing Methodology Conduct Wi-Fi penetration testing to attempt handshake capture and unauthorized access. Analyze signal coverage.

Compliance Criteria

- WPA3-Enterprise or stronger in use.
- Rogue APs are detected and reported within 10 minutes.

Evaluation Methods Deploy rogue devices and validate response. Inspect authentication server logs and detection tools.

2.15 System and Information Integrity (SI) CCIs

2.15.1 CCI-002605: Flaw Remediation Policy and Procedures

Assessment Procedures Review the organization's policy on identifying, reporting, and correcting software and system flaws. Interview administrators to understand the patch prioritization process and response timelines.

Evidence Requirements

- Flaw remediation policies and SOPs.
- Vulnerability management workflow documentation.
- Patch deployment schedules and audit trails.

Testing Methodology Introduce a known critical CVE into a non-production system and track the remediation response. Review SLA adherence on remediation timelines.

Compliance Criteria

- Critical flaws remediated within defined SLA (e.g., 7 days).
- Documented processes exist for zero-day vulnerabilities.

Evaluation Methods Match real patch deployment records to vulnerability discovery dates. Interview IT and security staff on manual vs. automated patch handling.

2.15.2 CCI-002607: Patch Deployment Testing Procedures

Assessment Procedures Inspect the organization's process for testing patches before deployment. Evaluate rollback capabilities and pre-deployment validation methods.

Evidence Requirements

- Patch test reports and rollback documentation.
- Staging environment test cases and results.
- Change control board approvals.

Testing Methodology Review a recent patch applied in production and verify that it underwent testing in a staging environment. Attempt rollback to prior state in a test environment.

Compliance Criteria

- 100% of patches tested before production deployment.
- Rollback procedures documented and validated quarterly.

Evaluation Methods Review changelogs and version control history. Interview QA and DevOps teams on test coverage and risk classification.

2.15.3 CCI-004996: Integrity Verification Tools for Software and Firmware

Assessment Procedures Inspect deployment of integrity verification tools (e.g., Tripwire, AIDE) on critical components. Confirm routine checks and alerting mechanisms.

Evidence Requirements

- Integrity monitoring tool configurations and logs.
- Scheduled scan results showing hash baseline comparisons.
- Alerts or incident reports from detected modifications.

Testing Methodology Introduce minor changes to monitored files in a test environment. Confirm that alerts are triggered and logged.

Compliance Criteria

- All critical system binaries and config files are monitored.
- Alerts generated for any unauthorized file modifications.

Evaluation Methods Examine baseline hashes and change detection rules. Interview system administrators on response to integrity alerts.

2.15.4 CCI-004997: Integrity Checks on Software and Firmware

Assessment Procedures Evaluate how frequently integrity checks are conducted and the scope of files being validated. Review automated check schedules and trigger conditions.

Evidence Requirements

- Cron jobs or automation scripts for integrity checks.
- Logs from recent verification scans.
- Configuration files showing targeted files/directories.

Testing Methodology Corrupt or replace a test binary and validate detection. Check whether the alert is escalated through the appropriate channel.

Compliance Criteria

- Integrity checks run at least weekly on critical assets.
- Detection of anomalies results in log entries and alerts.

Evaluation Methods Review logs and escalation records. Compare integrity tool coverage with critical asset inventory.

2.15.5 CCI-002710: System Monitoring Policy and Procedures

Assessment Procedures Review the policy governing system monitoring, including covered components, frequency, and alert thresholds. Confirm procedures for responding to flagged activity.

Evidence Requirements

- System monitoring policies.
- SIEM platform configuration documentation.
- Response playbooks and incident reports.

Testing Methodology Generate sample anomalous behavior (e.g., failed login attempts) and trace it through logs and alerts. Observe SOC handling of the event.

Compliance Criteria

- Monitoring is continuous for all production systems.
- Alerts are correlated, categorized, and addressed per SOP.

Evaluation Methods Analyze log aggregation and alert routing configurations. Interview SOC analysts on real-time incident workflows.

2.15.6 CCI-002711: Detection of Unauthorized Connections or Devices

Assessment Procedures Inspect tools used to detect rogue or unauthorized devices on the network. Validate network access control policies and scanning mechanisms.

Evidence Requirements

- Network access control (NAC) policy.
- Logs from port security, NAC, or rogue device alerts.
- Reports of past unauthorized connection detections.

Testing Methodology Attempt to connect an unauthorized device to a secure network port or wireless SSID. Monitor alert response.

Compliance Criteria

- All unauthorized devices detected within 5 minutes.
- Alerts logged and escalated automatically.

Evaluation Methods Audit detection coverage using NAC reports. Interview networking staff on tuning and response protocols.

2.15.7 CCI-002712: Detection of Unauthorized Use of System Resources

Assessment Procedures Review configurations for detecting abnormal resource usage, privilege escalations, or process anomalies. Confirm alerting thresholds are appropriate for normal activity baselines.

Evidence Requirements

- Logs from host-based intrusion detection systems (HIDS).
- Resource usage baselines and anomaly detection policies.
- Incident response tickets for resource misuse.

Testing Methodology Simulate unauthorized use (e.g., high CPU from unknown process). Observe HIDS/EDR detection and alert generation.

Compliance Criteria

- Alerts are triggered for privilege escalation or system abuse.
- SOC response within defined SLA (e.g., 30 minutes).

Evaluation Methods Review alert history and analyst responses. Perform live anomaly tests in a sandbox.

3 Test Cases

3.1 Critical CCI Test Cases

This section provides an example of what test cases for critical CCIs identified should look like. The table below outlines specific tests, procedures, and expected results.

CCI ID	Test Description	Test Procedure	Expected Result
CCI-000213	Account Creation Approval Verification	Attempt to create a new user account in the X9 UAV system without submitting proper approval documentation through the designated workflow.	The system rejects the account creation request, displaying an error message indicating missing approval.
CCI-000213	Inactive Account Disablement	Create a test account in the X9 UAV system and leave it inactive for more than 30 days, monitoring system behavior over time.	The account is automatically disabled after 30 days of inactivity, as verified by access denial and updated account status logs.
CCI-000831	Automatic Shutdown on Security Violation	Simulate three consecutive failed authentication attempts on the X9 UAV Ground Control Station (GCS) within a controlled test environment.	The system shuts down within 5 seconds of the third failed attempt, with logs confirming the shutdown trigger and timing.

Table 1: Critical CCI Test Cases

These test cases focus on critical security controls related to account management and incident response, ensuring the system's resilience against unauthorized access and security violations.

3.2 Testing Tools and Environments

The following tools and environments are utilized to conduct the CCI assessments for the X9 UAV system:
Testing Tools:

- **Nessus Vulnerability Scanner**: Identifies security weaknesses in system components, including firmware and software.
- **Wireshark**: Analyzes network traffic to verify encryption and detect anomalies in UAV-GCS communications.
- **Custom UAV Simulation Software**: Simulates flight operations and communication protocols specific to the X9 UAV.
- **Automated Test Scripts**: Executes functional and regression tests for consistent and repeatable results.
- **Penetration Testing Tools (e.g., Metasploit)**: Simulates attacks to assess system defenses against real-world threats.

Testing Environments:

- **Isolated Lab Environment**: A controlled setting for simulating UAV operations without external interference, ensuring safety and repeatability.

- **Virtual Machines**: Sandboxed environments for testing Ground Control Station (GCS) software, allowing rapid deployment and rollback.
- **Hardware-in-the-Loop (HIL) Setup**: Integrates physical UAV hardware with simulated inputs to test firmware and real-time responses.

These tools and environments enable comprehensive testing across software, hardware, and network layers of the X9 UAV system.

4 Documentation Requirements

4.1 Required Documentation

The following documentation is required to demonstrate compliance with the assessed CCIs for the X9 UAV system:

- **System Security Plan (SSP)**: Details the system's security controls, boundaries, and implementation status.
- **Incident Response Plan**: Outlines procedures for detecting, responding to, and recovering from security incidents.
- **Configuration Management Plan**: Describes processes for managing and documenting system configuration changes.
- **Access Control Policy**: Defines rules and procedures for granting, modifying, and revoking system access.
- **Audit Logs and Reports**: Records of system activities and security events, including timestamps and actions.
- **Vulnerability Scan Reports**: Results from regular scans, detailing identified weaknesses and remediation status.
- **Penetration Test Reports**: Findings from simulated attacks, including exploited vulnerabilities and mitigation steps.
- **Training Records**: Documentation of security training provided to administrators and users.
- **Approval Signatures**: Signed approvals for policies, plans, and significant system changes.

These documents provide a comprehensive record of compliance and system security posture.

4.2 Documentation Templates

Templates for key compliance documents should include the following structures:

- **System Security Plan Template**: Based on NIST SP 800-18, including sections for system identification, security categorization, control implementation details, and risk assessment results.
- **Incident Response Plan Template**: Covers incident detection, analysis, containment, eradication, recovery, and post-incident lessons learned, with predefined roles and responsibilities.
- **Test Report Template**: Documents test objectives, methodologies, detailed results, and compliance status for each assessed CCI, with sections for findings and recommendations.

These templates streamline documentation efforts and ensure consistency across submissions.

4.3 Documentation Standards

All compliance documentation must adhere to the following standards:

- **Format**: Documents must be submitted in PDF format to ensure consistency and prevent unauthorized modifications.
- **Version Control**: Each document must include a version number and change log to track revisions and updates over time.

- **Approval**: Documents require signatures from authorized personnel (e.g., system owner, security officer) to indicate official approval.
- **Storage**: Documentation must be stored in a secure, access-controlled repository, with role-based access enforced to prevent unauthorized access or tampering.

These standards ensure that documentation is secure, traceable, and meets audit requirements.