**DMV Administrative Hearings Management System**

November 16, 2022

**Security Evaluation Form (SEf)**

Version 1.6

Prepared for

**North Carolina Department of Information Technology - Transportation**



**Executive Summary**

The State of North Carolina Statewide Information Security Manual (SISM) was established by the State CIO under authority N.C.G.S § 143B-1375, 143B-1376, and 143B-1378 to identify and implement information technology security controls. The policies, guidelines, and standards established by the SISM apply to all [Information Environments](https://csrc.nist.gov/glossary/term/information_environment) that store, process, transmit, and/or can impact the security of NCDOT/DMV data.

**STATUTORY LAW**

<https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1375.pdf>

<https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1376.pdf>

<https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-1378.pdf>

**POLICIES, GUIDELINES AND STANDARDS**

<https://it.nc.gov/resources/cybersecurity-and-risk-management/esrmo-initiatives/statewide-information-security/>

<https://it.nc.gov/documents/statewide-data-classification-and-handling-policy>

<https://archives.ncdcr.gov/government/state-government-agencies/functional-schedule>

**Glossary of Information Technology Terms**

<https://it.nc.gov/documents/statewide-glossary-information-technology-terms>

<https://csrc.nist.gov/glossary>

**Purpose**

The Security Evaluation Form (SEF) and its underlying assessment activities serve to provide NCDOT with an understanding of the third-party contractor’s [security capabilities](https://csrc.nist.gov/glossary/term/Security_Capability) relevant to the third-party contractor’s access to NCDOT’s [information resources](https://csrc.nist.gov/glossary/term/information_resources). The SEF is unlike a full [security assessment](https://csrc.nist.gov/glossary/term/security_assessment) in that the SEF typically does not require third-parties to submit technical evidence (e.g., screenshots, logs, packet captures, security scans, configuration exports, test results, etc.) to validate their stated security capabilities. This is important to understand because the third-party’s overall security capabilities are typically conceptual from NCDOT’s perspective and cannot be fully assessed and verified in a manner consistent with the Statewide Information Security Manual (SISM). For this reason, the outcome of this security evaluation is largely dependent on the third-party contractor’s ability to understand the security requirements established by NCDOT and provide meaningful and comprehensive responses to the questions in the SEF and throughout the assessment process.

**SECURITY CONTROLS AND CAPABILITIES**

The third-party contractor’s responses throughout the security evaluation are used to assess the third-party contractor’s overall security capabilities. Security capabilities are defined and evaluated by bringing together specific sets of security controls derived from the appropriately tailored baselines that together produce the required capabilities. The SISM establishes the security controls and capabilities that must be satisfied before [information systems](https://csrc.nist.gov/glossary/term/information_system) are permitted access to NCDOT’s data.

**Approach and Use of This Document**

The security evaluation begins when the third-party contractor returns their completed SEF and supporting documentation to NCDOT for review. In addition to the third-party contractor’s responses to the security questions, they may be asked to provide copies of their applicable security program documents including policies, standards, procedures, plans, dataflows, network architecture diagrams, third-party risk assessment reports, etc.

**Outcomes**

Submission of this report by the third-party does not guarantee a state-ready designation, nor does it guarantee that the North Carolina Department of Transportation (NCDOT) will procure services from the third-party.

**Third-Party’s System Information**

|  |
| --- |
| Third-Party Name:  System/Service Name:  Service Model: (e.g. IaaS, PaaS, SaaS)  FIPS PUB 199 System Security Level: (Moderate)  Fully Operational as of: Enter the date the system became fully operational.  Number of Customers (State/Others): Enter # of customers / # of other customers  Deployment Model: Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only Cloud, or Other? If other, please describe.  System Functionality: Briefly describe the functionality of the system and service being provided. |

|  |  |
| --- | --- |
| **Information Security Questionnaire** | |
| 1. The [Statewide Information Security Manual (SISM)](https://it.nc.gov/resources/cybersecurity-and-risk-management/esrmo-initiatives/statewide-information-security) was established by the State CIO under authority N.C.G.S § 143B-1375, 143B-1376, and 143B-1378. The policies and standards defined in the SISM apply to all systems and services that store, process, transmit, and/or could impact the security of NCDOT Data. It is important to understand a SOC 2 Type II (or equivalent) only indicates the third-party contractor’s policies, standards, and procedures were assessed as being compliant with generic industry accepted practices. A SOC 2 Type II (or equivalent) does not certify the third-party contractor’s services as being compliant with the NCDOT’s information security policies, guidelines, and standards (e.g., account lockout thresholds, employment background checks (local/State/Federal), minimum password requirements, data classification, change management, etc.). | |
| 1. The term **Personally Identifiable Information** **(PII)** refers to information that can be used to distinguish or trace an individual’s identity, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as name, date and place of birth, employer, home and work addresses, email address, phone number, mother’s maiden name, etc.   The third-party contractor’s services will process **Restricted** and/or **Highly Restricted** NCDOT data that could be used to distinguish or trace an individual’s identity. | |
| 1. Describe the third-party contractor’s methodology for acknowledging and maintaining compliance with NCDOT’s information security policies, guidelines, and standards. 2. Is the third-party contractor’s methodology documented in a policy document? 3. Does the methodology extend to all third parties supporting the third-party contractor’s services? Please explain in detail. | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. The **System Security Plan (SSP)** provides a summary of the security requirements of the [information system](https://csrc.nist.gov/glossary/term/information_system)(s) and describes the controls for meeting those requirements and defined responsibilities and expected behavior of all individuals who access the system. The SSP also contains or references other key security-related documents for the information system such as a risk assessment, Corrective Actions Plan (CAP), accreditation documentation, privacy threshold and impact assessment, contingency plan, configuration management plan, security configuration checklists and system interconnection agreements as appropriate. 2. Provide a System Security Plan (SSP) that addresses all applicable aspects of the third-party contractor’s proposed services and solution. Linked below is a copy of the State’s SSP template.   <https://it.nc.gov/documents/system-security-plan-template> | *If the third-party does not have an SSP, provides comprehensive response explaining how the third-party’s activities support the intent of the SSP. Please review the SSP template and understand the SISM requirements before responding.* |
| 1. **Data Flow Diagrams**: The purpose of a data flow diagram is to graphically represent data in all forms as it traverses systems including what changes the data and where it is stored at any given time. Examples of what could be represented in this diagram include data elements (name, address, phone, etc.), data format, encryption and compression, authentication, permissions, session, and registration (HTTP, SNMP, FTP, IRC, SSH, SSL, TLS, DES, 3-DES, AES, SSH, IMAP, RPC, SQL, NFS, API’s, Sockets and WinSock).    1. Provide data flow diagram(s) of the third-party contractor’s services. Attached is an example high-level data flow diagram. | *Provide a data flow diagram(s) that include all information systems that store, process, and/or transmit NCDOT/DMV data.*  *Please review the attachment and understand the intent of a data flow diagram before responding.* |
| 1. **Network Architecture Diagrams**: The purpose of network architecture diagrams is to graphically represent the structure of a network and shows the components that make up a network and how they interact, including routers, devices, hubs, firewalls, servers, workstations, printer, etc. 2. Provide network architecture diagrams of the third-party contractor’s services. | *Provide network architecture diagrams.* |
| 1. Does the third-party contractor have an external risk assessment report that demonstrates the third-party’s compliance to industry accepted guidelines (e.g., SOC 2 Type II, ISO 27001, FedRAMP, etc.) that addresses the scope of their proposed services?    1. Provide a copy of the third-party contractor’s external risk assessment report.    2. Describe in detail how the third-party contractor will ensure all external entities supporting the third-party’s proposed services receive and maintain SOC 2 Type II (or equivalent) certifications for their roles in supporting the third-party contractor’s proposed services and solution.    3. Does the third-party contractor have and maintain formal agreements with external entities, such as for maintenance and service support for the third-party contractor’s service?   **NOTE**: *It is important to understand a SOC 2 Type II (or equivalent) only indicates the third-party’s policies, standards, and procedures were assessed as being compliant with generic industry accepted guidelines. A SOC 2 Type II (or equivalent) does not certify the third-party’s services as being compliant with the State’s information security policies, guidelines, and standards (e.g., account lockout thresholds, employment background checks (local/State/Federal), minimum password requirements, data classification, change management, etc.). Third-party contractor must periodically perform formal security crosswalks between the third-party contractor’s policies/standards and the State’s policies/standards to ensure the proper security controls are in place to protect State data. (References: N.C.G.S § 143B-1375, § 143B-1378;* [*SISM PS-7*](https://it.nc.gov/documents/statewide-policies/scio-personnel-security/download?attachment)*,* [*CA-7*](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Security_Assessment_%26_Authorization.pdf)*,* [*RA-3*](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)*).* | *Provide a copy of the third-party’s risk assessment reports and provide responses to the questions in Section 7.*  *Please respond to sections i – iii.* |
| 1. Describe in detail how the third-party contractor’s proposed services support NCDOT’s **Multi‐factor authentication (MFA)** policy, guidelines, and standards. Specifically speak to Remote Access ([SISM AC-17](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), and Nonlocal Maintenance ([SISM MA-4](https://it.nc.gov/documents/statewide-policies/scio-maintenance/download?attachment)). 2. Do the third-party contractor’s services enforce MFA for all administrative functions? Explain in detail. 3. Do the third-party contractor’s services enforce MFA for all remote access to information systems that process State data? Explain in detail. | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.*  *Please respond to sections i and ii.* |
| 1. The **North Carolina Identity Management Service (NCID)** is the standard identity and access management platform provided by the Department of Information Technology. NCID is a web-based application that provides a secure environment for state agency, local government, business, and individual users to log in and gain access to real-time resources, such as customer-based applications and information retrieval.    1. Are the third-party contractor’s proposed services capable of integrating with the State’s NCID solution?    2. Describe in detail how the third-party contractor’s services integrate with the North Carolina Identity (NCID) Service.   **References:**  <https://it.nc.gov/ncid/>  <https://it.nc.gov/ncid-frequently-asked-questions>  <https://it.nc.gov/ncid-application-integration-requirements-airn-saml-based> | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Provide a list of all entities that support the third-party contractor’s services along with a detailed description of their roles and responsibilities. | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. All operating systems (OS) AND major application software components (e.g., Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must NOT be past N-1. Applications which are not operating on the most recent platform MUST have a roadmap to upgrade with a State approved timeline. 2. Do the third-party contractor’s proposed services support the State’s N-1 requirement? 3. Explain in detail how the third-party maintains the N-1 standard. | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Does the third-party contractor’s proposed services meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements? | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Does the third-party contractor’s services handle, store, process and/or transmit State [data](https://it.nc.gov/media/1797/open) outside the physical boundaries of the United States? If yes, explain in detail. | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required? Explain in detail.   The Statewide Data Classification and Handling Policy is located here:  <https://it.nc.gov/documents/statewide-policies/statewide-data-classification-handling-policy/open>  The Statewide Media Protection Policy is located here:  <https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Media_Protection.pdf> | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Do the third-party contractor’s services encrypt State data in-transit and at rest? Explain in detail. | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Do any information system components used by the third-party contractor to store, process, transmit, and/or can impact the security and privacy of NCDOT data use deprecated transport layer protocols (e.g., SSL, TLS 1.0, TLS 1.1)? 1.1)? Explain in detail. | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. State requires minimum 8-character complex passwords (Upper, Lower, Special Character and Numerical)? 2. Explain in detail how the third-party’s services enforce the State's password policy and standards (SISM [AC](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment), [IA](https://it.nc.gov/documents/statewide-policies/scio-identification-and-authentication/download?attachment), [MA](https://it.nc.gov/documents/statewide-policies/scio-maintenance/download?attachment), [SC](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment), [SI](https://it.nc.gov/documents/statewide-policies/scio-system-and-information-integrity/download?attachment), [SA](https://it.nc.gov/documents/statewide-policies/scio-system-and-service-acquisition/download?attachment)). | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the third-party contractor’s services detect, contain, and eradicate malicious software? [[SISM SI-3](https://it.nc.gov/documents/statewide-policies/scio-system-and-information-integrity/download?attachment), [SISM SI-3](https://it.nc.gov/documents/statewide-policies/scio-system-and-information-integrity/download?attachment), [SISM MA-3](https://it.nc.gov/documents/statewide-policies/scio-maintenance/download?attachment)] | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the third-party contractor’s services store audit data in a tamper-resistant manner and meets chain of custody and e-discovery requirements? [[SISM AU-7](https://it.nc.gov/documents/statewide-policies/scio-audit-accountability/download?attachment), [SISM AU-9](https://it.nc.gov/documents/statewide-policies/scio-audit-accountability/download?attachment)] | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the third-party contractor’s services detect unauthorized or malicious use of the systems, including insider threat and external intrusions? [[SISM SI-4](https://it.nc.gov/documents/statewide-policies/scio-system-and-information-integrity/download?attachment), [SISM SI-4 (4)](https://it.nc.gov/documents/statewide-policies/scio-system-and-information-integrity/download?attachment), [SISM SI-7](https://it.nc.gov/documents/statewide-policies/scio-system-and-information-integrity/download?attachment), [SISM SI-7 (7)](https://it.nc.gov/documents/statewide-policies/scio-system-and-information-integrity/download?attachment)] | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the third-party contractor performs security code analysis (static and dynamic) and evaluates code for security flaws, as well as identify, track, and remediate security flaws? [[SISM SA-11](https://it.nc.gov/documents/statewide-policies/scio-system-and-service-acquisition/download?attachment)] | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. Explain in detail how the third-party contractor’s records retention policy, standards, practices, and information systems adhere to the State’s functional records schedule. [[DNCR Functional Schedule](https://files.nc.gov/dncr-archives/documents/files/functional_overview_rev2019_final.pdf), [DNCR Information Technology](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf), [DNCR Risk Management](https://files.nc.gov/dncr-archives/documents/files/16_riskmgmt_final_rev2018.pdf), [SISM AU-7](https://it.nc.gov/documents/statewide-policies/scio-audit-accountability/download?attachment), [SISM AU-11](https://it.nc.gov/documents/statewide-policies/scio-audit-accountability/download?attachment)]?   A “[Record](https://files.nc.gov/ncdit/documents/files/Statewide-Glossary-2020.pdf)” is defined as a set of data (logical and physical) treated as a unit. Examples include, but are not limited to, IT Security Program documents, data flow and architecture diagrams, system/application diagrams, change management activities, risk management activities, vulnerability scan results, system/application logs, etc.   1. [**911.3** Data Documentation Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records concerning data in automated systems; includes data element dictionary, file layout, code book or table, Entity relationships tables, and other records related to the structure, management, and Entity of data  RETAIN UNTIL: System is discontinued and/or replaced  PLUS: 3 years  THEN: Destroy   1. [**914.<** Digitization and Scanning Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records concerning data entry and imaging operations; includes quality control records and paper records that are digitized.  RETAIN UNTIL: Digitized  PLUS: 10 days  THEN: Destroy NOTE: The digital surrogate becomes the record copy and must be retained according to the disposition instructions for that record type.   1. [**915.3** Electronic Records Policies](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records documenting the policies and procedures employed by the agency to maintain authentic and accessible electronic records.  RETAIN UNTIL: Superseded/Obsolete  PLUS: 3 years  THEN: Destroy   1. [**924.1(1)** Network and System Security Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records documenting the security of networks and systems; includes records concerning firewalls, anti-virus programs, and other related records.  RETAIN FROM: Creation  PLUS: 1 year  THEN: Destroy\*   1. [**924.1(2)** Network and System Security Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   records documenting access requests and authorizations, system access logs, and other related records  RETAIN FROM: Creation  PLUS: 1 year  THEN: Destroy   1. [**924.2** Network and System Security Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records documenting incidents involving unauthorized attempted entry or probes on data processing systems, information technology systems, telecommunications networks, and electronic security systems, including associated software and hardware; includes logs, extracts, compilations of data, and other related records  RETAIN FROM: Creation  PLUS: 2 years  THEN: Destroy\*   1. [**926.3** System Documentation](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   records documenting operating systems, application programs, structure and form of datasets, system structure, and system-to-system communication; includes system overviews, dataset inventories, server names, IP addresses, purpose of the systems, Entity-supplied documentation, installed software, and current source code.  RETAIN UNTIL: Superseded/Obsolete  PLUS: 3 years  THEN: Destroy   1. [**1623.3** Disaster Recovery Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records concerning minor or routine agency recovery operations that are managed with minimal disruption to normal operations  RETAIN UNTIL: Complete  PLUS: 3 years  THEN: Destroy   1. [**1314.2** Consultant, Contractor, Provider, and Entity Due Diligence Records](https://files.nc.gov/dncr-archives/documents/files/9_IT_final.pdf)   Records documenting the evaluation of consultants, contractors, providers, and entities with whom the agency conducts business; includes financial stability, information security risk assessments, and other related records  RETAIN UNTIL: Contract expires  PLUS: 2 years  THEN: Destroy | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.*  *Please explain in detail how the third-party’s services and solution support the SISM/DNCR requirements outlined in sections i – ix.* |
| 1. Does the third-party contractor have the capability to notify the State within 24 hours of suspected and/or confirmed incidents? Explain in detail. | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. If the third-party contractor’s services provide email “send as” capabilities, does it support DMARC and DKIM for email protection? If not, explain in detail. | *If the system does not support this feature, do not answer Y or N. Instead, state “Not Applicable” here.* |
| 1. Describe in detail how the third-party contractor’s services support NCDOT’s **Data Protection and Classification** policy, guidelines, and standards. Specifically speak to Security Impact Analysis ([SISM CM-4](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Media Protection Policy ([SISM MP-1](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Marking ([SISM MP-3](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Storage ([SISM MP-4](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Transport ([SISM MP-5](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Sanitization ([SISM MP-6](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Use ([SISM MP-7](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Prohibit Use Without Owner ([SISM MP-7(1)](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Security Categorization ([SISM RA-2](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), and the Statewide Data Classification Policy. | *Describe in detail how the third-party’s proposed services and solution supports NCDOT’s* ***Data Protection and Classification Policies****, guidelines, and standards.*  *Please address each of the SISM requirements listed in question #25 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the third-party contractor’s services support NCDOT’s **Incident Response** policy, guidelines, and standards. Specifically speak to Incident Response Plan Testing ([SISM IR-3](https://it.nc.gov/documents/statewide-policies/scio-incident-response/download?attachment)), Incident Response Plan Testing ([SISM IR-3(2)](https://it.nc.gov/documents/statewide-policies/scio-incident-response/download?attachment)), Incident Handling ([SISM IR-4](https://it.nc.gov/documents/statewide-policies/scio-incident-response/download?attachment)), Incident Monitoring ([SISM IR-5](https://it.nc.gov/documents/statewide-policies/scio-incident-response/download?attachment)), Incident Reporting ([SISM IR-6](https://it.nc.gov/documents/statewide-policies/scio-incident-response/download?attachment)), and Incident Response Plan ([SISM IR-8](https://it.nc.gov/documents/statewide-policies/scio-incident-response/download?attachment)). | *Describe in detail how the third-party’s proposed services and solution supports NCDOT’s Incident Response policy, guidelines, and standards.*  *Please address each of the SISM requirements listed in question #26 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the third-party contractor’s services support NCDOT’s **Contingency Planning** policy, guidelines, and standards. Specifically speak to Contingency Planning Policy ([SISM CP-1](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)), Contingency Plan ([SISM CP-2](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)), Contingency Plan Training ([SISM CP-3](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)), Contingency Plan Testing and Exercises ([SISM CP-4](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)), Contingency Plan Alternate Storage Site ([SISM CP-6](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)), Contingency Plan Alternate Processing Site ([SISM CP-7](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)), Information System Backup ([SISM CP-9](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)), Testing for Reliability/Integrity ([CP-9(1)](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)), and Information System Recovery and Reconstitution ([SISM CP-10](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)). 2. Describe in detail how the third-party contractor’s services recover the system(s) to a known and functional state following an outage, breach, DoS attack, or disaster? [[SISM CP-2](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment), [SISM CP-9](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment), [SISM CP-10](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)] 3. Do the third-party contractor’s services have alternate storage and processing facilities? [[SISM CP-6](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment), [SISM CP-7](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)]. If yes, explain in detail. 4. Does the third-party contractor have service level agreements (SLAs) in place with all third-party service providers including telecommunications providers? [[SISM CP-8](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)] 5. Describe in detail the third-party contractor’s information systems log recovery capabilities for each of the systems that handle, store, process, transmit, and/or can impact the security and privacy of NCDOT data? 6. Provide copies of the Business Impact Analysis (BIA) and Disaster Recovery Plan (DRP) for the third-party’s proposed services. Attached are templates. | *Describe in detail how the third-party’s proposed solution supports NCDOT’s* ***Contingency Planning*** *policy, guidelines, and standards and provide copies of the third-party’s PIA and BIA.*  *Please address each of the SISM requirements listed in question #27 in your response. Please review and understand the SISM requirements before responding.*  *Please respond to sections i – v.* |
| 1. Describe in detail how the third-party contractor’s services support NCDOT’s **Configuration Management** policy, guidelines, and standards. Specifically speak to Configuration Management Policy ([SISM CM-1](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Baseline Configuration ([SISM CM-2](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Configuration Change Control ([SISM CM-3](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Security Impact Analysis ([SISM CM-4](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Access Restrictions for Change ([SISM CM-5](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Configuration Settings ([SISM CM-6](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Least Functionality ([SISM CM-7](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Information System Component Inventory ([SISM CM-8](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Automated Unauthorized Component Detection ([SISM CM-8(3)](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Configuration Management Plan ([SISM CM-9](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Software Usage Restrictions ([SISM CM-10](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)), Separation of Duties ([SISM AC-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Remote Access ([SISM AC-17](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Access_Control.pdf)), Timely Maintenance ([SISM MA-6](https://it.nc.gov/documents/statewide-policies/scio-maintenance/download?attachment)), Continuous Monitoring ([SISM CA-7](https://it.nc.gov/documents/statewide-policies/scio-security-assessment-authorization/download?attachment)), Flaw Remediation ([SISM SI-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_System_and_Information_Integrity.pdf)), Malicious Code Protection ([SISM SI-3](https://it.nc.gov/documents/statewide-policies/scio-system-and-information-integrity/download?attachment)), System Development Life Cycle ([SISM SA-3](https://it.nc.gov/documents/statewide-policies/scio-system-and-service-acquisition/download?attachment)), and Developer Configuration Management ([SISM SA-10](https://it.nc.gov/documents/statewide-policies/scio-system-and-service-acquisition/download?attachment)). 2. Provide a copy of the third-party contractor’s Change Management Policy, Standards and Procedures. 3. Provide a copy of the third-party contractor’s Configuration Management Plan, Policy, Standards and Procedures. 4. Does the third-party contractor’s change management capability include a fully functioning Change Advisory Boards (CAB)/ Technical Review Boards (TRB)? 5. Does the third-party contractor have and use development and/or test environments to verify changes before implementing them in the production environment? 6. Within the third-party contractor’s proposed solution, are all products and services still actively supported? 7. Does the third-party contractor have a lifecycle management plan that ensures products are updated before they reach the end of life? 8. Provide a copy of the third-party contractor’s Security Impact Analysis (SIA) for the third-party’s proposed solution. Below is a Security Impact Analysis template ([SISM CM-4](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)). | *Describe in detail how the third-party’s proposed services and solution supports NCDOT’s* ***Configuration Management*** *policy, guidelines, and standards.*  *Please address each of the SISM requirements listed in question #28 in your response. Please review and understand the SISM requirements before responding.*  *Please respond to sections i – vii.* |
| 1. Describe in detail how the third-party contractor’s services support NCDOT’s **System and Communications Protection** policy, guidelines, and standards. Specifically speak to Policy ([SISM SC-1](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), Application Partitioning ([SISM SC-2](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), Information in Shared Resources ([SISM SC-4](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), Denial of Service Protection ([SISM SC-5](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), Boundary Protection ([SISM SC-7](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), Transmission Confidentiality and Integrity ([SISM SC-8](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), Network Disconnect ([SISM SC-10](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), Cryptographic Key Establishment and Management ([SISM SC-12](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), Cryptographic Protection ([SISM SC-13](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), Public Key Infrastructure Certificates ([SISM SC-17](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)), and Mobile Code ([SISM SC-18](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)). | *Describe in detail how the third-party’s proposed services and solution supports NCDOT’s* ***System and Communications Protection*** *policy, guidelines, and standards.*  *Please address each of the SISM requirements listed in question #29 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the third-party contractor’s services support NCDOT’s **Identification & Authentication** policy, guidelines, and standards. Specifically speak to Access Control ([SISM AC-1](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Account Management ([SISM AC-2](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Automated System Account Management ([SISM AC-2(1)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Removal of Temporary / Emergency Accounts ([SISM AC-2(2)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Disable Inactive Accounts ([SISM AC-2(3)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Automated Audit Actions ([SISM AC-2(4)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Access Enforcement ([SISM AC-3](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Information Flow Enforcement ([SISM AC-4](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Separation of Duties ([SISM AC-5](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Least Privilege ([SISM AC-6](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Unsuccessful Logon Attempts ([SISM AC-7](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), System Use Notification ([SISM AC-8](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Session Lock ([SISM AC-11](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Pattern-Hiding Displays ([SISM AC-11(1)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment), Session Termination ([SISM AC-12](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Remote Access ([SISM AC-17](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Remote Access Automated Monitoring / Control (SISM [AC-17(1)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Remote Access – Protection of Confidentiality / Integrity Using Encryption ([SISM AC-17(2)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Remote Access – Managed Access Control Points ([SISM AC-17(3)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Remote Access – Privileged Commands / Access ([SISM AC-17(4)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Access Control for Mobile Devices ([SISM AC-19](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Access Control for Mobile Devices – Full Device / Container- Based Encryption ([SISM AC-19(5)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Use of External Information Systems ([SISM AC-20](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Use of External Information Systems – Limits on Authorized Use ([SISM AC-20(1)](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), Information Sharing ([SISM AC-21](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)), and Publicly Accessible Content ([SISM AC-22](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)). | *Describe in detail how the third-party’s proposed services and solution supports NCDOT’s* ***Identification & Authentication*** *policy, guidelines, and standards.*  *Please address each of the SISM requirements listed in question #30 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the third-party’s services support NCDOT’s **Media Protection** policy, guidelines, and standards. Specifically speak to Policy ([SISM MP-1](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Access ([SISM MP-2](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Marking ([SISM MP-3](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Storage ([SISM MP-4](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Transport ([SISM MP-5](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Sanitization ([SISM MP-6](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), Media Use ([SISM MP-7](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)), and Media Use – Prohibit Use Without Owner ([SISM MP-7(1)](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)). | *Describe in detail how the third-party’s proposed services and solution supports NCDOT’s* ***Media Protection*** *policy, guidelines, and standards*.  *Please address each of the SISM requirements listed in question #31 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the third-party contractor’s services support NCDOT’s **Personnel Security** policy, guidelines, and standards. Specifically speak to Policy ([SISM PS-1](https://it.nc.gov/documents/statewide-policies/scio-personnel-security/download?attachment)), Position Risk Designation ([SISM PS-2](https://it.nc.gov/documents/statewide-policies/scio-personnel-security/download?attachment)), Personnel Screening ([SISM PS-3](https://it.nc.gov/documents/statewide-policies/scio-personnel-security/download?attachment)), Personnel Termination ([SISM PS-4](https://it.nc.gov/documents/statewide-policies/scio-personnel-security/download?attachment)), Personnel Transfer ([SISM PS-5](https://it.nc.gov/documents/statewide-policies/scio-personnel-security/download?attachment)), Access Agreements ([SISM PS-6](https://it.nc.gov/documents/statewide-policies/scio-personnel-security/download?attachment)), and Third-Party Personnel Security ([SISM PS-7](https://it.nc.gov/documents/statewide-policies/scio-personnel-security/download?attachment)). | *Describe in detail how the third-party’s proposed services and solution supports NCDOT’s* ***Personnel Security*** *policy, guidelines, and standards.*  *Please address each of the SISM requirements listed in question #32 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the third-party contractor’s services support NCDOT’s **Risk Assessment** policy, guidelines, and standards. Specifically speak to Policy ([SISM RA-1](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Security Categorization ([SISM RA-2](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Risk Assessment ([SISM RA-3](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Vulnerability Scanning ([SISM RA-5](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Vulnerability Scanning – Update Tool Capability ([SISM RA-5(1)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), Vulnerability Scanning – Frequency of Updates ([SISM RA-5(2)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)), and Vulnerability Scanning – Privileged Access ([SISM RA-5(5)](https://files.nc.gov/ncdit/documents/Statewide_Policies/SCIO_Risk_Assessment.pdf)). | *Describe in detail how the third-party’s proposed services and solution supports NCDOT’s* ***Risk Assessment*** *policy, guidelines, and standards.*  *Please address each of the SISM requirements listed in question #33 in your response. Please review and understand the SISM requirements before responding.* |
| 1. Describe in detail how the third-party contractor’s services support NCDOT’s **Physical & Environmental Protection** policy, guidelines, and standards. Specifically speak to Policy ([SISM PE-1](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Physical Access Authorizations ([SISM PE-2](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Physical Access Control ([SISM PE-3](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Access Control for Transmission Medium ([SISM PE-4](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Access Control for Output Devices ([SISM PE-5](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Monitoring Physical Access ([SISM PE-6](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Monitoring Physical Access – Intrusion Alarms ([SISM PE-6(1)](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Visitor Access Records ([SISM PE-8](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Power Equipment and Cabling ([SISM PE-9](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Emergency Power ([SISM PE-11](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Fire Protection ([SISM PE-13](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Fire Protection – Automatic Fire Suppression ([SISM PE-13(3)](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Delivery and Removal ([SISM PE-16](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), Alternate Work Site ([SISM PE-17](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)), and Location of Information System Components ([SISM PE-18](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)). | *Describe in detail how the third-party’s proposed services and solution supports NCDOT’s* ***Physical & Environmental Protection*** *policy, guidelines, and standards.*  *Please address each of the SISM requirements listed in question #34 in your response. Please review and understand the SISM requirements before responding.* |
| 1. When Critical or High software vulnerability are identified and patching is not an option, what **Continuous Monitoring** activities does the third-party perform to maintain visibility and identify if the known vulnerabilities been exploited? 2. How does the third-party contractor track known vulnerabilities that cannot be remediated? 3. Submit a Corrective Actions Plan (CAP) that identifies all third-party contractor vulnerabilities and security controls that do not comply with or meet the intent of the security requirements established in the State of North Carolina Statewide Information Security Manual (SISM).   The CAP template can be found here:  <https://it.nc.gov/documents/files/corrective-action-plan-template-v1/open>  The CAP instructions can be found here:  <https://it.nc.gov/documents/files/corrective-action-plan-instructions/open> | *Third-party provides a comprehensive response here. Please review and understand the SISM requirements before responding.* |
| 1. **Policies, Procedures, and Training**   The third-party contractor must indicate the status of their policies, standards, and procedures coverage.  To answer “**Yes**” to a policy, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance. A single policy document may address more than one family provided the requirements of each “1” are fully addressed.  Third-party contractors must establish their own set of policies, standards, and procedures. They cannot be inherited from a leveraged system or service provider. Any exceptions and/or missing policy and procedure elements must be explained in comments section. | |

| **Family** | **Policy** | | **Standards** | | **Procedures** | | **Document Title, Version, and Last Review Date** | **Comments** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Yes** | **No** | **Yes** | **No** | **YES** | **No** |
| Access Control  [[SISM AC-1](https://it.nc.gov/documents/statewide-policies/scio-access-control/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Awareness & Training  [[SISM AT-1](https://it.nc.gov/documents/statewide-policies/scio-security-awareness-training/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Audit & Accountability [[SISM AU-1](https://it.nc.gov/documents/statewide-policies/scio-audit-accountability/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Security Assessment & Authorization  [[SISM CA-1](https://it.nc.gov/documents/statewide-policies/scio-system-and-service-acquisition/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Configuration Management  [[SISM CM-1](https://it.nc.gov/documents/statewide-policies/scio-configuration-management/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Contingency Planning  [[SISM CP-1](https://it.nc.gov/documents/statewide-policies/scio-contingency-planning/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Identification & Authentication  [[SISM IA-1](https://it.nc.gov/documents/statewide-policies/scio-identification-and-authentication/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Incident Response  [[SISM IR-1](https://it.nc.gov/documents/statewide-policies/scio-incident-response/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Maintenance  [[SISM MA-1](https://it.nc.gov/documents/statewide-policies/scio-maintenance/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Media Protection  [[SISM MP-1](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Physical & Environmental Protection  [[SISM PE-1](https://it.nc.gov/documents/statewide-policies/scio-physical-and-environmental-protection/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Personnel Security  [[SISM PS-1](https://it.nc.gov/documents/statewide-policies/scio-personnel-security/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Risk Assessment  [[SISM RA-1](https://it.nc.gov/documents/statewide-policies/scio-risk-assessment/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| System & Services Acquisition  [[SISM SA-1](https://it.nc.gov/documents/statewide-policies/scio-system-and-service-acquisition/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| System & Communications Protection  [[SISM SC-1](https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| System & Information Integrity  [[SISM SI-1](https://it.nc.gov/documents/statewide-policies/scio-system-and-information-integrity/download?attachment)] |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |
| Planning  [[SISM PL-1]](https://it.nc.gov/documents/statewide-policies/scio-security-planning/download?attachment) |  |  |  |  |  |  | Policy:  Standards:  Procedures: |  |