Nebraska Standard Title	Nebraska Standard Reference	NIST 800-171 Reference	NIST 800-171 Group	NIST 800-171 Description
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.7 ITS-02-4.1.10	3.1.20	ACCESS CONTROL	Verify and control/limit connections to and use of external systems.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.2	3.1.9	ACCESS CONTROL	Provide privacy and security notices consistent with applicable CUI rules.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.3 ITS-02-4.2.1 ITS-02-4.2.5	3.5.1	IDENTIFICATION AND AUTHENTICATION	Identify system users, processes acting on behalf of users, and devices.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.3 ITS-02-4.2.1 ITS-02-4.2.5 ITS-02-4.6.1	3.5.2	IDENTIFICATION AND AUTHENTICATION	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.4	3.1.5	ACCESS CONTROL	Employ the principle of least privilege, including for specific security functions and privileged accounts.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.5	3.1.4	ACCESS CONTROL	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.6	3.1.1	ACCESS CONTROL	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.7	3.1.21	ACCESS CONTROL	Limit use of portable storage devices on external systems.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.7	3.1.15	ACCESS CONTROL	Authorize remote execution of privileged commands and remote access to security-relevant information.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.1.7	3.1.18	ACCESS CONTROL	Control connection of mobile devices.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.2.2	3.1.6	ACCESS CONTROL	Use non-privileged accounts or roles when accessing nonsecurity functions
ITS-02 Access Identification and Authentication Standard	ITS-02-4.2.4	3.5.3	IDENTIFICATION AND AUTHENTICATION	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.2.6	3.1.11	ACCESS CONTROL	Terminate (automatically) a user session after a defined condition.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.2.6 ITS-02-4.2.9	3.1.10	ACCESS CONTROL	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.2.7	3.1.7	ACCESS CONTROL	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.3.2	3.1.2	ACCESS CONTROL	Limit system access to the types of transactions and functions that authorized users are permitted to execute
ITS-02 Access Identification and Authentication Standard	ITS-02-4.4.1	3.1.13	ACCESS CONTROL	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions
ITS-02 Access Identification and Authentication Standard	ITS-02-4.4.1	3.1.19	ACCESS CONTROL	Encrypt CUI on mobile devices and mobile computing platforms.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.4.2	3.1.3	ACCESS CONTROL	Control the flow of CUI in accordance with approved authorizations.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.4.2	3.1.14	ACCESS CONTROL	Route remote access via managed access control points.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.4.2	3.1.22	ACCESS CONTROL	Control CUI posted or processed on publicly accessible systems.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.4.3	3.1.8	ACCESS CONTROL	Limit unsuccessful logon attempts.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.4.3	3.1.12	ACCESS CONTROL	Monitor and control remote access sessions.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.5.1	3.1.16	ACCESS CONTROL	Authorize wireless access prior to allowing such connections.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.5.1, ITS-02-4.5.2	3.1.17	ACCESS CONTROL	Protect wireless access using authentication and encryption.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.6.2	3.5.11	IDENTIFICATION AND AUTHENTICATION	Obscure feedback of authentication information.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.6.3	3.5.4	IDENTIFICATION AND AUTHENTICATION	Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.6.4	3.5.5	IDENTIFICATION AND AUTHENTICATION	Prevent reuse of identifiers for a defined period.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.2.9 ITS-02-4.6.4	3.5.6	IDENTIFICATION AND AUTHENTICATION	Disable identifiers after a defined period of inactivity
ITS-02 Access Identification and Authentication Standard	ITS-02-4.7.3	3.5.10	IDENTIFICATION AND AUTHENTICATION	Store and transmit only cryptographically-protected passwords
ITS-02 Access Identification and Authentication Standard	ITS-02-4.7.4	3.5.9	IDENTIFICATION AND AUTHENTICATION	Allow temporary password use for system logons with an immediate change to a permanent password.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.7.5	3.5.7	IDENTIFICATION AND AUTHENTICATION	Enforce a minimum password complexity and change of characters when new passwords are created.
ITS-02 Access Identification and Authentication Standard	ITS-02-4.7.6	3.5.8	IDENTIFICATION AND AUTHENTICATION	Prohibit password reuse for a specified number of generations.
ITS-03 Asset Management Standard ITS-06 Configuration Management Standard	ITS-03-4.2.3 ITS-06-4.1.1	3.4.1	CONFIGURATION MANAGEMENT	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
ITS-04 Audit and Accountability Standard	ITS-04-4.1.1	3.3.2	AUDIT AND ACCOUNTABILITY	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.
ITS-04 Audit and Accountability Standard	ITS-04-4.1.2	3.3.1	AUDIT AND ACCOUNTABILITY	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

ITS-04 Audit and Accountability Standard	ITS-04-4.1.2	3.3.3	AUDIT AND ACCOUNTABILITY	Review and update logged events.
ITS-04 Audit and Accountability Standard	ITS-04-4.1.3	3.3.4	AUDIT AND ACCOUNTABILITY	Alert in the event of an audit logging process failure.
ITS-04 Audit and Accountability Standard	ITS-04-4.2.1	3.3.7	AUDIT AND ACCOUNTABILITY	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
ITS-04 Audit and Accountability Standard	ITS-04-4.3.1	3.3.8	AUDIT AND ACCOUNTABILITY	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
ITS-04 Audit and Accountability Standard	ITS-04-4.3.2	3.3.9	AUDIT AND ACCOUNTABILITY	Limit management of audit logging functionality to a subset of privileged users.
ITS-04 Audit and Accountability Standard	ITS-04-4.4.1	3.3.5	AUDIT AND ACCOUNTABILITY	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
ITS-04 Audit and Accountability Standard	ITS-04-4.4.2	3.3.6	AUDIT AND ACCOUNTABILITY	Provide audit record reduction and report generation to support on-demand analysis and reporting.
ITS-05 Awareness and Training Standard	ITS-05-4.1.1	3.2.1	AWARENESS AND TRAINING	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
ITS-05 Awareness and Training Standard	ITS-05-4.1.3	3.2.3	AWARENESS AND TRAINING	Provide security awareness training on recognizing and reporting potential indicators of insider threat.
ITS-05 Awareness and Training Standard	ITS-05-4.1.4	3.2.2	AWARENESS AND TRAINING	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
ITS-06 Configuration Management Standard	ITS-06-4.1.2	3.4.6	CONFIGURATION MANAGEMENT	Employ the principle of least functionality by configuring organizational systems to provideonly essential capabilities.
ITS-06 Configuration Management Standard	ITS-06-4.1.3	3.4.8	CONFIGURATION MANAGEMENT	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
ITS-06 Configuration Management Standard	ITS-06-4.1.3	3.4.9	CONFIGURATION MANAGEMENT	Control and monitor user-installed software.
ITS-06 Configuration Management Standard	ITS-06-4.2.1	3.4.2	CONFIGURATION MANAGEMENT	Establish and enforce security configuration settings for information technology products employed in organizational systems.
ITS-06 Configuration Management Standard	ITS-06-4.2.2	3.4.5	CONFIGURATION MANAGEMENT	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
ITS-06 Configuration Management Standard	ITS-06-4.2.3	3.4.7	CONFIGURATION MANAGEMENT	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
ITS-06 Configuration Management Standard	ITS-06-4.2.4 ITS-06-4.2.5 ITS-06-4.2.6	3.4.3	CONFIGURATION MANAGEMENT	Track, review, approve or disapprove, and log changes to organizational systems.
ITS-06 Configuration Management Standard	ITS-06-4.2.7	3.4.4	CONFIGURATION MANAGEMENT	Analyze the security impact of changes prior to implementation.
ITS-07 Incident Response Standard	ITS-07-4.3.1 ITS-07-4.3.2 ITS-07-4.3.3	3.6.2	INCIDENT RESPONSE	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
ITS-07 Incident Response Standard ITS-12 Recovery Standard	ITS-07-4.1.1 ITS-07-4.1.2 ITS-07-4.2.1 ITS-07-4.2.2 ITS-07-4.2.3 ITS-07-4.4.1 ITS-12.4.1.3 ITS-12.4.1.4	3.6.1	INCIDENT RESPONSE	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
ITS-07 Incident Response Standard ITS-12 Recovery Standard	ITS-07-4.5.1 ITS-12.4.1.5	3.6.3	INCIDENT RESPONSE	Test the organizational incident response capability.
ITS-08 Systems Maintenance Standard	ITS-08.4.1.1	3.7.1	MAINTENANCE	Perform maintenance on organizational systems.
ITS-08 Systems Maintenance Standard	ITS-08.4.1.2	3.7.2	MAINTENANCE	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
ITS-08 Systems Maintenance Standard	ITS-08.4.1.2	3.7.4	MAINTENANCE	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
ITS-08 Systems Maintenance Standard	ITS-02-4.4.3 ITS-08.4.1.3	3.7.5	MAINTENANCE	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
ITS-08 Systems Maintenance Standard	ITS-08.4.1.4	3.7.6	MAINTENANCE	Supervise the maintenance activities of maintenance personnel without required access authorization.
ITS-08 Systems Maintenance Standard	ITS-08.4.1.6	3.7.3	MAINTENANCE	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
ITS-09 Media and Protection Standard	ITS-09.4.2.3	3.8.7	MEDIA PROTECTION	Control the use of removable media on system components.
ITS-09 Media and Protection Standard	ITS-09.4.2.3	3.8.8	MEDIA PROTECTION	Prohibit the use of portable storage devices when such devices have no identifiable owner.
ITS-09 Media and Protection Standard	ITS-09.4.3.1 ITS-09.4.5.1	3.8.1	MEDIA PROTECTION	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
ITS-09 Media and Protection Standard	ITS-09.4.3.1 ITS-09.4.5.1	3.8.2	MEDIA PROTECTION	Limit access to CUI on system media to authorized users.
ITS-09 Media and Protection Standard	ITS-09.4.6.1	3.8.3	MEDIA PROTECTION	Sanitize or destroy system media containing CUI before disposal or release for reuse.
ITS-09 Media and Protection Standard	ITS-09.4.7.1	3.8.5	MEDIA PROTECTION	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

ITS-09 Media and Protection Standard	ITS-09.4.7.1	3.8.6	MEDIA PROTECTION	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
ITS-09 Media and Protection Standard	ITS-09-4.1.1 ITS-09-4.2.1 ITS-09-4.2.2	3.8.4	MEDIA PROTECTION	Mark media with necessary CUI markings and distribution limitations.
ITS-09 Media and Protection Standard ITS-12 Recovery Standard	ITS-09.4.3.1 ITS-09.4.5.1 ITS-12.4.1.6 ITS-12.4.1.7	3.8.9	MEDIA PROTECTION	Protect the confidentiality of backup CUI at storage locations.
ITS-10 Personnel Security Standard	ITS-10-4.1.1 ITS-10-4.1.2 ITS-10-4.1.3	3.9.1	PERSONNEL SECURITY	Screen individuals prior to authorizing access to organizational systems containing CUI.
ITS-10 Personnel Security Standard	ITS-10-4.2.1 ITS-10-4.2.2	3.9.2	PERSONNEL SECURITY	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
ITS-11 Physical Protection Standard	ITS-11-4.1.11	3.10.5	PHYSICAL PROTECTION	Control and manage physical access devices.
ITS-11 Physical Protection Standard	ITS-11-4.1.12	3.10.6	PHYSICAL PROTECTION	Enforce safeguarding measures for CUI at alternate work sites.
ITS-11 Physical Protection Standard	ITS-11-4.1.2	3.10.1	PHYSICAL PROTECTION	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
ITS-11 Physical Protection Standard	ITS-11-4.1.4	3.10.2	PHYSICAL PROTECTION	Protect and monitor the physical facility and support infrastructure for organizational systems.
ITS-11 Physical Protection Standard	ITS-11-4.1.7	3.10.3	PHYSICAL PROTECTION	Escort visitors and monitor visitor activity.
ITS-11 Physical Protection Standard	ITS-11-4.1.7	3.10.4	PHYSICAL PROTECTION	Maintain audit logs of physical access.
ITS-13 Risk Management Standard	ITS-13-4.1.1 ITS-13-4.2.1	3.11.1	RISK ASSESSMENT	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
ITS-13 Risk Management Standard	ITS-13-4.3.1	3.11.2	RISK ASSESSMENT	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
ITS-13 Risk Management Standard	ITS-13-4.3.2	3.11.3	RISK ASSESSMENT	Remediate vulnerabilities in accordance with risk assessments.
ITS-14 Security Assessment Standard	ITS-14-4.1.1 ITS-14-4.1.2	3.12.4	SECURITY ASSESSMENT	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
ITS-14 Security Assessment Standard	ITS-14-4.1.1 ITS-14-4.3.2	3.12.3	SECURITY ASSESSMENT	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
ITS-14 Security Assessment Standard	ITS-14-4.3.1 ITS-14-4.3.2 ITS-14-4.3.3	3.12.1	SECURITY ASSESSMENT	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
ITS-14 Security Assessment Standard	ITS-14-4.3.2 ITS-14-4.3.3	3.12.2	SECURITY ASSESSMENT	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
ITS-16 System and Communications Protection Standard	ITS-16-4.1.1	3.13.5	SYSTEM AND COMMUNICATIONS PROTECTION	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
ITS-16 System and Communications Protection Standard	ITS-16-4.1.2	3.13.6	SYSTEM AND COMMUNICATIONS PROTECTION	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
ITS-16 System and Communications Protection Standard	ITS-16-4.1.6	3.13.9	SYSTEM AND COMMUNICATIONS PROTECTION	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
ITS-16 System and Communications Protection Standard	ITS-16-4.1.7	3.13.15	SYSTEM AND COMMUNICATIONS PROTECTION	Protect the authenticity of communications sessions.
ITS-16 System and Communications Protection Standard	ITS-16-4.1.8	3.13.7	SYSTEM AND COMMUNICATIONS PROTECTION	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
ITS-16 System and Communications Protection Standard	ITS-16-4.1.9	3.13.14	SYSTEM AND COMMUNICATIONS PROTECTION	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
ITS-16 System and Communications Protection Standard	ITS-16-4.4.1 ITS-16-4.4.2 ITS-16-4.4.3	3.13.2	SYSTEM AND COMMUNICATIONS PROTECTION	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
ITS-16 System and Communications Protection Standard	ITS-16-4.4.3	3.13.12	SYSTEM AND COMMUNICATIONS PROTECTION	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
ITS-16 System and Communications Protection Standard	ITS-16-4.4.4	3.13.3	SYSTEM AND COMMUNICATIONS PROTECTION	Separate user functionality from system management functionality.

ITS-16 System and Communications Protection Standard	ITS-16-4.4.5	3.13.13	SYSTEM AND COMMUNICATIONS PROTECTION	Control and monitor the use of mobile code.
ITS-16 System and Communications Protection Standard	ITS-16-4.4.6	3.13.4	SYSTEM AND COMMUNICATIONS PROTECTION	Prevent unauthorized and unintended information transfer via shared system resources.
ITS-16 System and Communications Protection Standard	ITS-16-4.5.2	3.13.16	SYSTEM AND COMMUNICATIONS PROTECTION	Protect the confidentiality of CUI at rest.
ITS-16 System and Communications Protection Standard	ITS-16-4.5.3	3.13.8	SYSTEM AND COMMUNICATIONS PROTECTION	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
ITS-16 System and Communications Protection Standard	ITS-16-4.5.4 ITS-16-4.5.5 ITS-16-4.5.6 ITS-16-4.5.7 ITS-16-4.5.8	3.13.10	SYSTEM AND COMMUNICATIONS PROTECTION	Establish and manage cryptographic keys for cryptography employed in organizational systems.
ITS-16 System and Communications Protection Standard	ITS-16-4.5.8	3.13.11	SYSTEM AND COMMUNICATIONS PROTECTION	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
ITS-16 System and Communications Protection Standard ITS-17 System and Informational Integrity Standard	ITS-16-4.1.3 ITS-17-4.2.6 ITS-17-4.3.1 ITS-17-4.3.2	3.13.1	SYSTEM AND COMMUNICATIONS PROTECTION	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
ITS-17 System and Informational Integrity Standard	ITS-17-4.1.1 ITS-17-4.1.2 ITS-17-4.1.4	3.14.1	SYSTEM AND INFORMATION INTEGRITY	Identify, report, and correct system flaws in a timely manner.
ITS-17 System and Informational Integrity Standard	ITS-17-4.1.1 ITS-17-4.1.2 ITS-17-4.1.4	3.14.3	SYSTEM AND INFORMATION INTEGRITY	Monitor system security alerts and advisories and take action in response.
ITS-17 System and Informational Integrity Standard	ITS-17-4.2.1 ITS-17-4.2.2	3.14.6	SYSTEM AND INFORMATION INTEGRITY	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
ITS-17 System and Informational Integrity Standard	ITS-17-4.2.1 ITS-17-4.2.2	3.14.7	SYSTEM AND INFORMATION INTEGRITY	Identify unauthorized use of organizational systems.
ITS-17 System and Informational Integrity Standard	ITS-17-4.2.4	3.14.2	SYSTEM AND INFORMATION INTEGRITY	Provide protection from malicious code at designated locations within organizational systems
ITS-17 System and Informational Integrity Standard	ITS-17-4.2.4	3.14.4	SYSTEM AND INFORMATION INTEGRITY	Update malicious code protection mechanisms when new releases are available.
ITS-17 System and Informational Integrity Standard	ITS-17-4.2.5	3.14.5	SYSTEM AND INFORMATION INTEGRITY	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.