Orbital ATK

NIST 800-171 Control #	Security Control Category	Control Name	Assessment Question	Select Control Maturity *Selection Must Be Made	Describe how the Control is implemented. If control is Defined, Repeatable, or Initial describe any corrective action being taken. (Include the technology involved if applicable)	Provide Completion Date of Any Corrective Action Plans (Ex. 1/11/2016)	Other Notes
3.1.1, 3.1.2	ACCESS CONTROL	ACCOUNT MANAGEMENT	Are there processes in place to ensure access provided to users (e.g., the role provided to a user for an application, or privileged access provided to an IT administrator, etc.) aligns with business requirements and/or access control policy? [Note: an example could be documented approval from asset/business owner, timely removal of access from transferred or terminated employees, etc.].				
3.1.1, 3.1.2	ACCESS CONTROL	ACCESS ENFORCEMENT	Are information systems (applications, operating systems, network devices, databases, etc.) configured and access enforcement mechanisms employed per approved policy to provide protection from unauthorized access by malicious users, software or systems?				
3.1.4	ACCESS CONTROL	SEPARATION OF DUTIES	Are there identified, documented, and separated duties of individuals (or roles) as necessary to prevent collusion or fraud If so, has such separation of duties been implemented through assigned information system access authorizations? [Note: Fraud could occur when: administrator has ability to clear system logs; developers have update access to production systems; application roles where individual with access to accounts payable has access to cash accounts, etc.]				
3.1.5	ACCESS CONTROL	LEAST PRIVILEGE	Are there established and implemented procedures to restrict system access to only authorized personnel based on need to know and to other information systems based on business function requirements? [Note the organization may need to control access to facilities, information inside applications, software programs for testing and revision.]				
3.1.8	ACCESS CONTROL	UNSUCCESSFUL LOGON ATTEMPTS	Are there procedures and controls to lock user access to information resources after a defined number of unsuccessful login attempts?				
3.1.9	ACCESS CONTROL	SYSTEM USE NOTIFICATION	Is there an information systems display outlining an approved system use notification message or banner before granting access to the information system?				
3.1.10	ACCESS CONTROL	SESSION LOCK	Does the information system enforce automatic session time-out after a pre-determined / reasonable period of inactivity (e.g., 10 minutes)?				
3.1.1, 3.1.2	ACCESS CONTROL	REMOTE ACCESS	Are there policies and processes in place for: (i) providing secure remote access to information systems, including rules on when privileged access is provided, (ii) monitoring and authorizing remote access to information systems, and (iii) enforcing requirements for remote connections to the information system in place? [Note: Documentation on methods should also include usage restrictions and implementation guidance for each allowed remote access method; secure remote connections include proper configuration and use of encryption; example of privileged remote access include approval(s) required based on business need, and use of stronger authentication such as two-factor].				
3.1.18	ACCESS CONTROL	ACCESS CONTROL FOR MOBILE DEVICES	Are there documented policies, standards, and procedures in place for addressing and enforcing security related to usage of mobile devices (e.g., USB drives, PDAs, Smart Phones, tablets, etc.), including Bring Your Own Device (BYOD)? [Note: Example controls include: policies that define how such devices are used in context of business; and technical controls such as password requirements to access the device, use of "containers" to segregate confidential information, use of encryption on containers, remote wipe-out capabilities for PDAs/Smartphones, etc.]				
3.1.20	ACCESS CONTROL	USE OF EXTERNAL INFORMATION SYSTEMS	Is there an institutional or departmental policy and supporting processes that require information security be considered as part of due diligence, contracting, and risk monitoring for third-parties that manage, store, or process, confidential information on behalf of the institution or department (e.g., SaaS , outsourced data center, ASP, cloud services, etc.)?				

3.1.22	ACCESS CONTROL	PUBLICLY ACCESSIBLE CONTENT	Is there a defined policy and supporting process for sharing / posting institutional information in the public domain (e.g., website, externally accessible systems)?				
3.2.1, 3.2.2	AWARENESS AND TRAINING	SECURITY AWARENESS TRAINING	Is there on-going basic security awareness training to all information system users (including department heads, senior executives, and contractors)?				
3.2.1, 3.2.2	AWARENESS AND TRAINING	SECURITY AWARENESS TRAINING	Is there targeted training in place for positions with higher risk profile (e.g., system administrators, personnel with access to student records, etc.?				
3.3.1, 3.3.2	AUDIT AND ACCOUNTABILITY	CONTENT OF AUDIT RECORDS	Does the information system produce audit records that contain sufficient information and, at a minimum, establish: a. the type of event that occurred, b. the date and time the event occurred, c. where the event occurred, (Specific system, etc.) d. the source of the event, e. outcome (success or failure) of the event, and f. the identity of any user or subject associated with the event?				
3.3.1, 3.3.2	AUDIT AND ACCOUNTABILITY	AUDIT REVIEW, ANALYSIS, AND REPORTING	Are information system audit records reviewed and analyzed on a daily basis for indications of inappropriate or unusual activity, findings reported to designated organizational officials, and corrective action plans implemented for identified issues? [e.g., logs from different system correlated in order to effectively detect potential security issues; specific use cases for alerts been defined in order to identify critical security events; there are knowledgeable resources that exist and are responsible for responding to alerts; such process is tied to the incident response process]				
3.3.8	AUDIT AND ACCOUNTABILITY	PROTECTION OF AUDIT INFORMATION	Is access to log data directories adequately controlled?				
3.3.1, 3.3.2	AUDIT AND ACCOUNTABILITY	AUDIT GENERATION	Is there a documented logging standard that defines the minimum requirements for logging (e.g., fields to log, type of events, log protection requirements, retention requirements, etc.)?				
3.12.1, 3.12.2, 3.12.3	SECURITY ASSESSMENT AND AUTHORIZATION	SECURITY ASSESSMENTS	Is there a defined information security program that includes: i) developing a plan and executing periodic assessments of security control effectiveness; ii) identifying objective and qualified assessors; and iii) reporting results of such assessment(s) to the appropriate stakeholders?				
3.12.1, 3.12.2, 3.12.3	SECURITY ASSESSMENT AND AUTHORIZATION	CONTINUOUS MONITORING	Is there a continuous monitoring program that includes configuration management, ongoing security control assessments, and reporting on the information system and its constituent components?				
3.4.1, 3.4.2	CONFIGURATION MANAGEMENT	BASELINE CONFIGURATION	Are there established and communicated minimum baseline security configuration standards for information systems accessing institutional networks using baseline security standards based on some recognized or industry guidance (e.g., vendor documentation, CIS (Center for Internet Security), NIST, etc.)?				
3.4.3	CONFIGURATION MANAGEMENT	CONFIGURATION CHANGE CONTROL	Are changes to baseline security configuration standards managed, tested, and approved by a formally defined change management function that includes representation from appropriate stakeholders?				
3.4.1, 3.4.2	CONFIGURATION MANAGEMENT	CONFIGURATION SETTINGS	Are there processes in place to monitor and control changes to the baseline configuration settings of information systems in accordance with organizational policies and procedures?				
3.4.6	CONFIGURATION MANAGEMENT	LEAST FUNCTIONALITY	Do the configuration management procedures include processes for providing only essential functionality and restrict the use of functionality, ports, protocols, and/or services based on risk?				
3.4.1, 3.4.2	CONFIGURATION MANAGEMENT	INFORMATION SYSTEM COMPONENT INVENTORY	Is there a current and accurate inventory of systems, that provides details such as associated owners, location, security requirements, data classification, etc., for the department?				
3.5.1, 3.5.2	IDENTIFICATION AND AUTHENTICATION	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	Are strong authentication controls (e.g., two-factor authentication and proper encryption of credentials) in place for administrative type access to information system(s)?				

3.5.5, 3.5.6	IDENTIFICATION AND AUTHENTICATION	IDENTIFIER MANAGEMENT	Does the company manage information system identifiers for users and devices by receiving authorization from a designated official to assign a unique user identifier (user-id), preventing reuse of user-ids, and disabling user-ids to information resources and data under their authority?				
3.5.1, 3.5.2	IDENTIFICATION AND AUTHENTICATION	AUTHENTICATOR MANAGEMENT	Are there established, documented, and implemented administrative procedures to manage information system authenticators such as passwords, key fobs, certificates, etc., for users and information systems, and ensure user identity when issuing or resetting them? [e.g., establishing and implementing administrative procedures for initial authenticator distribution; changing default content of authenticators upon information system installation, etc., as per institution requirement].				
3.6.1, 3.6.2	INCIDENT RESPONSE	INCIDENT RESPONSE TRAINING	Is there incident management training that is suitable and relevant to the individual's role, responsibilities and skills?				
3.6.1, 3.6.2	INCIDENT RESPONSE	INCIDENT HANDLING	Does the company review the incident response plan and procedures at defined intervals taking into account lessons learned, industry best practices, and alignment with other processes, as applicable (e.g., breach notifications, crisis management, etc.)?				
3.6.1, 3.6.2	INCIDENT RESPONSE	INCIDENT RESPONSE ASSISTANCE	Is there access, or means of obtaining access quickly, to skilled incident response support (e.g., to perform forensics) during an incident? [Note: examples may include forensic specialists in other parts of the institution or executed contracts in place with third-parties that provide such capability]				
3.7.1, 3.7.2, 3.7.3	MAINTENANCE	CONTROLLED MAINTENANCE	Are there documented and implemented policies and practices for maintaining proper security of information system hardware (e.g., hard drives removed from servers, printers, fax machines, etc.) as well as physical facilities such as doors, locks, etc., during maintenance, whether on-site or when removed and taken off-site?				
3.7.1, 3.7.2	MAINTENANCE	MAINTENANCE TOOLS	Are there documented and implemented policies and processes for limiting security risk exposure through maintenance or diagnostic tools (e.g., an unpatched and unsecure device or appliance connected to the network etc.) introduced into the institution by third-parties?				
3.7.5	MAINTENANCE	NONLOCAL MAINTENANCE	Are there documented and implemented policies and practices to control security exposure from institutional vendors who provide remote support or maintenance to information system(s), through: i) enabling strong identification and authentication; ii) limiting to ports, services, and access levels needed for business purpose; iii) having appropriate logging enabled for monitoring vendor actions; and iv) session termination of sessions and network connections when remote maintenance is completed?				
3.7.6	MAINTENANCE	MAINTENANCE PERSONNEL	Are there documented policies and practices for preventing visitors from physically accessing sensitive areas of the institution through: i) use of physical controls such as locked doors; ii) requiring management authorization for non-employees or visitors to enter facilities; iii) issuance of a physical token (e.g., badge or access device) that expires and that identifies the individual as a non-employee; iv) use of sign-in sheets or automated visitor logging; v) maintenance of records of visits based on institutional records retention schedules?				
3.8.1, 3.8.2, 3.8.3	MEDIA PROTECTION	MEDIA ACCESS	Are there administrative, physical, and technical controls in place to manage access to media containing confidential information?				
3.8.1, 3.8.2, 3.8.3	MEDIA PROTECTION	MEDIA STORAGE	Are there media handling procedures to address: i) proper storage and physical security of digital and non-digital media (e.g., backup tapes, student & patient records, etc.); ii) destruction or sanitization of media using approved equipment, techniques, and procedures; and iii) other requirements for media handling based on any institution or department's data classification scheme?				
3.8.5	MEDIA PROTECTION	MEDIA TRANSPORT	Are there procedures to protect media in transit which include logging and monitoring media transfers, encryption of confidential data, and use of secured couriers? [Note: a common example of media in transit can include backup tapes, mobile devices like laptops and PDAs].				

3.8.7	MEDIA PROTECTION	MEDIA USE	Are there documented policies and supporting processes to restrict unauthorized information system media within its environment?				
3.8.9	MEDIA PROTECTION	INFORMATION SYSTEM BACKUP	Does the company backup user-level and system-level information, system documentation, and security-related documentation consistent with recovery objectives and protect the confidentiality and integrity of backups?				
3.10.1, 3.10.2	PHYSICAL AND ENVIRONMENTAL PROTECTION	PHYSICAL ACCESS AUTHORIZATIONS	Are there established roles and does it enforce associated access requirements of institutional facilities that house systems and confidential data based on business requirements or function? (e.g., where student or patient records are maintained) based on business requirements or function? [Note: this is about formally defining and enforcing who can access a specific facility based on business needs].				
3.10.3, 3.10.4, 3.10.5	PHYSICAL AND ENVIRONMENTAL PROTECTION	PHYSICAL ACCESS CONTROL	Are there appropriate processes in place to control designated entry/exit points of areas where confidential information or critical systems are maintained through: i) a formal authorization process for providing access credentials (badge, key, code, etc.); ii) a process to revoke access (e.g., due to termination or change of job role) to the facility; iii) protecting the system that manages control for entry/exit (e.g., restricting system access to the badge system); and iv) monitoring for events that indicate potential unauthorized access attempts to the facility (e.g., unsuccessful badge attempts, loss of physical key, etc.)?				
3.10.1, 3.10.2	PHYSICAL AND ENVIRONMENTAL PROTECTION	ACCESS CONTROL FOR OUTPUT DEVICES	Are there documented and implemented physical safeguards to protect sensitive documents and/or output devices (e.g., special forms, negotiable instruments, special-purpose printers or security tokens)?				
3.9.1, 3.9.2	PERSONNEL SECURITY	PERSONNEL SCREENING	Are there implemented processes that require Human Resources to screen potential employees and contractors prior to being hired in order to minimize the risk of attacks from internal sources?				
3.9.1, 3.9.2	PERSONNEL SECURITY	PERSONNEL TERMINATION	Are there documented policies and supporting processes in place to: i) promptly revoke/disable access of employees, contractors, etc., upon termination; and ii) retrieve all security-related institutional information and system-related property (e.g., institutionally provided laptops, PDAs, access cards, keys, etc.)?				
3.9.1, 3.9.2	PERSONNEL SECURITY	PERSONNEL TRANSFER	Are there processes in place to timely update access to information resources and facilities due to changes in role of the employee or contractor?				
3.11.1	RISK ASSESSMENT	RISK ASSESSMENT	Are information security risk assessments conducted at least annually?				
3.11.2, 3.11.3	RISK ASSESSMENT	VULNERABILITY SCANNING	Does the company have tools or other capability (e.g., third-party service providers), and processes in place for conducting security vulnerability scanning that includes: i) executing scans on a scheduled basis for its information systems (e.g., servers, network devices, databases, applications, workstations, wireless scans, etc.); ii) evaluating and reporting scan results to the appropriate stakeholders; iii) remediating vulnerabilities based on risk; and iv) sharing information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the institution to help eliminate similar vulnerabilities in other information systems, i.e., systemic weaknesses or deficiencies?				
3.13.1, 3.13.2	SYSTEM AND COMMUNICATIONS PROTECTION	SECURITY ENGINEERING PRINCIPLES	Does the company have system security engineering principles embedded into its System Development Lifecycle (SDLC) to achieve the goal of "secure by design" when building, customizing, and/or purchasing information systems (e.g., applications, servers, etc.)? [Note: example of engineering principles could include use of "Input Validation Library" for web applications to reduce exposure from vulnerabilities from input manipulation (e.g., SQL injection)].				

3.13.3	SYSTEM AND COMMUNICATIONS PROTECTION	APPLICATION PARTITIONING	Are there policies and supporting processes to segregate administrative / management tools and consoles from general user/application traffic? [Note: examples include segmenting the network into security zones where administrative interfaces and systems are separate from other system areas; use of ACLs and stronger authentication for accessing administrative functions, etc.].				
3.13.4	SYSTEM AND COMMUNICATIONS PROTECTION	INFORMATION IN SHARED RESOURCES	Are there policies and supporting processes in place to reduce risk of exposure of confidential data through shared system or multi-tenant (cloud) environments? (For example, often a single instance of a database is used to support multiple applications with different security risk profiles, and exposure from one application may expose the data of the other application)				
3.13.1, 3.13.2, 3.13.5	SYSTEM AND COMMUNICATIONS PROTECTION	BOUNDARY PROTECTION	Are there effective mechanisms (i.e., tools and processes) in place for monitoring and controlling network traffic at the perimeter (either at the institution level and/or security zones within the institution or department)? If Yes, do they include: i) properly placed and configured firewalls, proxies, and other security appliances; ii) use of and gateways that inspect incoming and outgoing network traffic; and iii) security baselines for such devices and periodic review of configured rules?				
3.13.8	SYSTEM AND COMMUNICATIONS PROTECTION	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	1) Does the company employ cryptographic mechanisms (e.g., digital signature) to recognize changes to information during transmission unless otherwise protected by alternative physical measures?				
3.13.9	SYSTEM AND COMMUNICATIONS PROTECTION	NETWORK DISCONNECT	Are information systems configured in a manner that custodians can, in accordance with the institution's policy, terminate network connections associated with a communication session and "kill" the session in a manner that someone else cannot hijack or take over a session neither i) at the end of the session, nor ii) after a period of inactivity?				
3.13.11	SYSTEM AND COMMUNICATIONS PROTECTION	CRYPTOGRAPHIC PROTECTION	Are there policies and supporting processes in place that provide requirements on: i) situations where encryption should be applied; and ii) use of appropriate level of encryption strengths based on current practices, and in compliance with State and Federal requirements?				
3.13.15	SYSTEM AND COMMUNICATIONS PROTECTION	SESSION AUTHENTICITY	Does the company have a control in place to protect the authenticity of communications sessions? [Note: For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the institution (e.g., sessions in service-oriented architectures providing web-based services).]				
3.13.16	SYSTEM AND COMMUNICATIONS PROTECTION	PROTECTION OF INFORMATION AT REST	Does the company provide controls for the protection of confidentiality and integrity of information at rest. [Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Institutions may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate]				
3.14.1, 3.14.2, 3.14.3	SYSTEM AND INFORMATION INTEGRITY	FLAW REMEDIATION	Are there policies and supporting processes for timely identification and implementation of patches to applicable information systems (e.g., operating systems, applications, databases, etc.) based on risk? [Note: An organization may consider applying a risk-based approach to prioritize their patch installations.]				
3.14.1, 3.14.2, 3.14.3, 3.14.4, 3.14.5	SYSTEM AND INFORMATION INTEGRITY	MALICIOUS CODE PROTECTION	Are there policies, supporting processes and measures for guarding against, detecting, and reporting malicious software (e.g., anti-virus, anti-spyware, etc.) across applicable information systems like servers and endpoints? [Note: processes include ensuring that tools are properly deployed across applicable information systems mechanisms, as well as regularly updating rules, signature, and behavior patterns, etc.]				

3.14.6, 3.14.7	SYSTEM AND INFORMATION INTEGRITY	INFORMATION SYSTEM MONITORING	1) Are there effective tools and processes in place to proactively detect and respond to security threats/events, through: i) effectively placed and configured intrusion-detection system(s) and/or intrusion-prevention system(s) to guard against or monitor for malicious network traffic at the perimeter; ii) effective placement and use of monitoring tools with configured applicable use cases to detect potential events relevant to the information system (e.g., DLP, SIEM, Netflow, etc.) ; iii) effective monitoring processes (e.g., alerts from IDS/IPS alert) for taking timely actions; iv) defined processes (e.g., use cases) that guide the responders to take appropriate level of action?				
3.14.1, 3.14.2, 3.14.3	SYSTEM AND INFORMATION INTEGRITY	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	Does the company receive and provide, timely security notifications and advisories to appropriate institution personnel (e.g., security advisories from external sources to institutional or departmental administrators; general security advisories like a phishing scam to institutional users)?				