EMRY NETWORKS
IT Solutions That Click

FREE WORKSHEET · NIST SP 800-171 · SPRS · EMRY NETWORKS | DEFENSIBLE IT

NIST SP 800-171 SPRS Score Worksheet

A printable self-assessment aid for small defense suppliers. All 110 NIST SP 800-171 Rev. 2 requirements with their DoD Assessment Methodology (v1.2.1) point values. Prepared by **Emry Networks** | (603) 202-3200 | Book a 30-Minute Risk Assessment

WHAT'S INSIDE

●	How the score works, assessment details and disclaimer	p. 2
1	Worksheet: all 110 requirements with DoD point values	p. 3
2	Score tally and points deducted by family	p. 9
●	Sources	p. 10

JUMP TO A FAMILY

Access Control	p. 3	Media Protection	p. 6
Awareness and Training	p. 4	Personnel Security	p. 6
Audit and Accountability	p. 4	Physical Protection	p. 6
Configuration Management	p. 4	Risk Assessment	p. 6
Identification and Authentication	p. 5	Security Assessment	p. 7
Incident response	p. 5	System and Communications Protection	p. 7
Maintenance	p. 5	System and Information Integrity	p. 8

Book a 30-Minute Risk Assessment →

Prefer to do it online? Use the SPRS Score Calculator: it keeps your answers in your browser and builds the same score.

USING THE INTERACTIVE VERSION

- **Pick a Status for every requirement** from the blue-outlined drop-downs. Press Tab to move to the next box.
- **Grey boxes calculate themselves:** the points off on each row, your estimated SPRS score, the counts and the points deducted by family.
- **Best in Adobe Acrobat Reader (free)** or another desktop PDF app. Browser viewers and Apple Preview let you type, but may not run the calculations; you can type those values in yourself.
- **Use the links** in the contents list, the header (Contents, Results) and the bookmarks panel to jump around.
- **Save often.** Prints on US Letter, landscape; the on-screen buttons do not print.

Print worksheet | Clear all entries

STATUS KEY

- **Met**: The requirement is implemented today.
- **Not Met**: Subtracts the full DoD value.
- **Partial**: Only on 3.5.3 and 3.13.11 (subtracts 3).
- **N/A - not permitted**: Only on 3.1.12, 3.1.13, 3.1.16, 3.1.17 and 3.1.18 (no points subtracted).

How the score works

DoD Assessment Methodology v1.2.1

- Start at **110**. For every requirement not met, subtract its DoD value (5, 3 or 1). The lowest possible score is **-203**.
- Partial credit exists only for **3.5.3** (MFA: subtract 3 if MFA covers remote and privileged users but not general users; 5 if no MFA) and **3.13.11** (subtract 3 if encryption is used but not FIPS-validated; 5 if no encryption where required). Anywhere else, partly done counts as not met.
- **3.12.4** (system security plan) has no point value, but without an SSP the DoD says an assessment cannot be completed.
- **3.1.12, 3.1.13, 3.1.16, 3.1.17, 3.1.18:** do not subtract points if remote access, wireless access or mobile device connection is not permitted; keep a policy that prevents it being enabled.
- A plan of action does not turn a gap into a Met. Only a temporary deficiency that arises after implementation and is tracked in a plan of action may be scored as implemented.
- In SPRS you post the summary score, assessment date, SSP scope and CAGE codes, and the date you expect to reach 110, not the line-by-line values.

Assessment details

Company / CAGE code(s)		**Assessment date**	
SSP name / version		**Assessor**	

Disclaimer

This worksheet is a self-assessment aid, not legal advice and not a certification. It does not replace the official DoD Assessment Methodology, NIST SP 800-171A assessment procedures, your contract terms, or advice from qualified counsel. The SPRS score you post is your company's representation to the government, so verify every answer against evidence before you submit it. Check both sources for updates. © 2026 Emry Networks.

1 Worksheet: all 110 requirements

NIST SP 800-171 Rev. 2 · DoD values: Annex A

Pick a Status for each row. Points off fills in automatically. Record evidence, or the POA&M action and owner, and a POA&M target date for every gap; the latest target date feeds the Score tally.

ID	Requirement (NIST SP 800-171 Rev. 2)	Pts	Status	Pts off	Evidence / POA&M action, owner	POA&M target date
Access Control						
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5				
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5				
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1				
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1				
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3				
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions	1				
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1				
3.1.8	Limit unsuccessful logon attempts.	1				
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	1				
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity	1				
3.1.11	Terminate (automatically) a user session after a defined condition.	1				
3.1.12	Monitor and control remote access sessions. Do not subtract points if remote access is not permitted (keep a policy that prevents it being enabled).	5				
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. Do not subtract points if remote access is not permitted (keep a policy that prevents it being enabled).	5				
3.1.14	Route remote access via managed access control points.	1				
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	1				
3.1.16	Authorize wireless access prior to allowing such connections Do not subtract points if wireless access is not permitted (keep a policy that prevents it being enabled).	5				
3.1.17	Protect wireless access using authentication and encryption Do not subtract points if wireless access is not permitted (keep a policy that prevents it being enabled).	5				
3.1.18	Control connection of mobile devices. Do not subtract points if connection of mobile devices is not permitted (keep a policy that prevents it being enabled).	5				

ID	Requirement (NIST SP 800-171 Rev. 2)	Pts	Status	Pts off	Evidence / POA&M action, owner	POA&M target date
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	3				
3.1.20	Verify and control/limit connections to and use of external systems.	1				
3.1.21	Limit use of portable storage devices on external systems.	1				
3.1.22	Control CUI posted or processed on publicly accessible systems.	1				
Awareness and Training						
3.2.1	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.	5				
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	5				
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	1				
Audit and Accountability						
3.3.1	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	5				
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	3				
3.3.3	Review and update logged events.	1				
3.3.4	Alert in the event of an audit logging process failure.	1				
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	5				
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	1				
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records	1				
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	1				
3.3.9	Limit management of audit logging functionality to a subset of privileged users.	1				
Configuration Management						
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	5				
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	5				
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	1				
3.4.4	Analyze the security impact of changes prior to implementation.	1				
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	5				

ID	Requirement (NIST SP 800-171 Rev. 2)	Pts	Status	Pts off	Evidence / POA&M action, owner	POA&M target date
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	5				
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	5				
3.4.8	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.	5				
3.4.9	Control and monitor user-installed software.	1				
Identification and Authentication						
3.5.1	Identify system users, processes acting on behalf of users, and devices.	5				
3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	5				
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. Partial = MFA implemented for remote and privileged users but not the general user (subtract 3). Not implemented for any users (subtract 5).	3 or 5				
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	1				
3.5.5	Prevent reuse of identifiers for a defined period.	1				
3.5.6	Disable identifiers after a defined period of inactivity.	1				
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	1				
3.5.8	Prohibit password reuse for a specified number of generations.	1				
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	1				
3.5.10	Store and transmit only cryptographically-protected passwords.	5				
3.5.11	Obscure feedback of authentication information	1				
Incident response						
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	5				
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	5				
3.6.3	Test the organizational incident response capability.	1				
Maintenance						
3.7.1	Perform maintenance on organizational systems.	3				
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	5				

ID	Requirement (NIST SP 800-171 Rev. 2)	Pts	Status	Pts off	Evidence / POA&M action, owner	POA&M target date
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	1				
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	3				
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	5				
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	1				
Media Protection						
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3				
3.8.2	Limit access to CUI on system media to authorized users	3				
3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	5				
3.8.4	Mark media with necessary CUI markings and distribution limitations.	1				
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	1				
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	1				
3.8.7	Control the use of removable media on system components.	5				
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	3				
3.8.9	Protect the confidentiality of backup CUI at storage locations.	1				
Personnel Security						
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	3				
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers	5				
Physical Protection						
3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	5				
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	5				
3.10.3	Escort visitors and monitor visitor activity.	1				
3.10.4	Maintain audit logs of physical access.	1				
3.10.5	Control and manage physical access devices.	1				
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	1				
Risk Assessment						

ID	Requirement (NIST SP 800-171 Rev. 2)	Pts	Status	Pts off	Evidence / POA&M action, owner	POA&M target date
3.11.1	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	**3**				
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	**5**				
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	**1**				
Security Assessment						
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	**5**				
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. Scored 'Not Met' if there is no plan of action for unimplemented requirements.	**3**				
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	**5**				
3.12.4	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. No point value. Without a system security plan, DoD says an assessment cannot be completed (noncompliance with DFARS 252.204-7012).	**NA**				
System and Communications Protection						
3.13.1	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.	**5**				
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	**5**				
3.13.3	Separate user functionality from system management functionality.	**1**				
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	**1**				
3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	**5**				
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	**5**				
3.13.7	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).	**1**				
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. Common-carrier MPLS separation is accepted without encryption (Methodology 5(i)(ii)).	**3**				
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	**1**				
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	**1**				
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. Partial = encryption employed but not FIPS-validated (subtract 3). No encryption employed where required (subtract 5).	**3 or 5**				

ID	Requirement (NIST SP 800-171 Rev. 2)	Pts	Status	Pts off	Evidence / POA&M action, owner	POA&M target date
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	1				
3.13.13	Control and monitor the use of mobile code.	1				
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	1				
3.13.15	Protect the authenticity of communications sessions.	5				
3.13.16	Protect the confidentiality of CUI at rest.	1				
System and Information Integrity						
3.14.1	Identify, report, and correct system flaws in a timely manner.	5				
3.14.2	Provide protection from malicious code at designated locations within organizational systems.	5				
3.14.3	Monitor system security alerts and advisories and take action in response.	5				
3.14.4	Update malicious code protection mechanisms when new releases are available.	5				
3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	3				
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	5				
3.14.7	Identify unauthorized use of organizational systems.	3				

2 Score tally

Calculated from the Worksheet

These totals fill in automatically from your answers in Adobe Acrobat Reader and most desktop PDF apps. If a box stays blank in your viewer, add up the Pts off column and type or write the numbers in. Unanswered rows are treated as Met. Do not post a score until all are answered.

B. Estimated SPRS summary score = 110 - A	A. Total points deducted	Requirements answered	Met	Not Met	Partial (3.5.3 / 3.13.11 credit only)	N/A - not permitted

A. Total points deducted (sum of the Pts off column)	
B. Estimated SPRS summary score = 110 - A	
Number of requirements Not Met / Partial	
3.12.4 SSP in place? (if No, there is no valid score)	
Plan of action completion date (date 110 expected)	

Points deducted by family

Family	Points deducted	Max possible deduction
Access Control		54
Awareness and Training		11
Audit and Accountability		19
Configuration Management		33
Identification and Authentication		27
Incident response		11
Maintenance		18

Family	Points deducted	Max possible deduction
Media Protection		23
Personnel Security		8
Physical Protection		14
Risk Assessment		9
Security Assessment		13
System and Communications Protection		42
System and Information Integrity		31

In SPRS you post the summary score, assessment date, SSP scope and CAGE codes, and the date you expect to reach 110, not the line-by-line values.

Prefer to do it online? Use the SPRS Score Calculator: it keeps your answers in your browser and builds the same score.

Sources

DoD NIST SP 800-171 Assessment Methodology v1.2.1 (point values: Annex A; rules: Section 5; SPRS format: Annex B): https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf
NIST SP 800-171 Rev. 2 (requirement text): https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
NIST SP 800-171A (assessment procedures): https://csrc.nist.gov/pubs/sp/800/171/a/final
DFARS 252.204-7019: https://www.acquisition.gov/dfars/252.204-7019-notice-nist-sp-800-171-dod-assessment-requirements.
DFARS 252.204-7020: https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.
SPRS reference: https://www.sprs.csd.disa.mil/reference.htm

Related Emry Networks resources

Companion guide: How SPRS scoring works (Emry Networks): https://www.emrynetworks.com/post/sprs-score-worksheet-nist-800-171
SPRS Score Calculator (online, free): https://www.emrynetworks.com/sprs-score-calculator

Want a second set of eyes before you post the score?

Emry Networks helps small defense suppliers build evidence-backed NIST SP 800-171 assessments. Call (603) 202-3200 or book a 30-Minute Risk Assessment.

Book a 30-Minute Risk Assessment →

Print worksheet
Clear all entries