AN OFFERING IN THE BLUE CYBER SERIES:

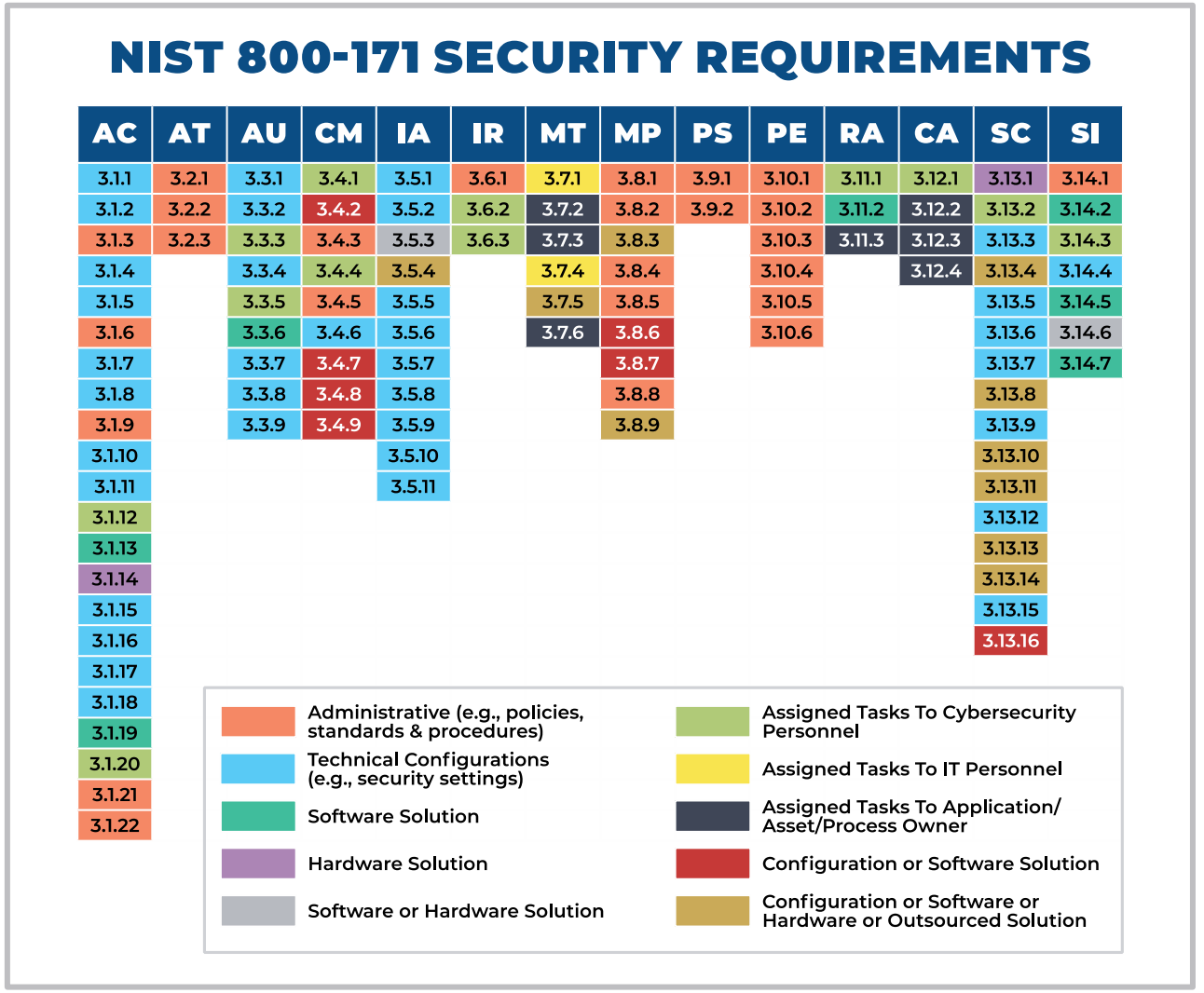
Questions to Ask When Choosing Cybersecurity Services

Version 14 March 2022

#14 in the Blue Cyber Education Series

NISP SP 800-171 Requirements

Link to the NIST SP 800-171 Requirements document: www.csrc.nist.gov/publications/detail/sp/800-171/rev-2/final



Begin in the Board Room

- Go back to the Blue Cyber "**Where to Begin with NIST SP 800-171**"
  - Decide where Cybersecurity fits in your business architecture
    - What does your business system look like?
    - Where does the Information System fit?
    - Who is responsible for the Information System?
    - What is the budget?
    - What level of risk are you comfortable with?

...Still in the Board Room

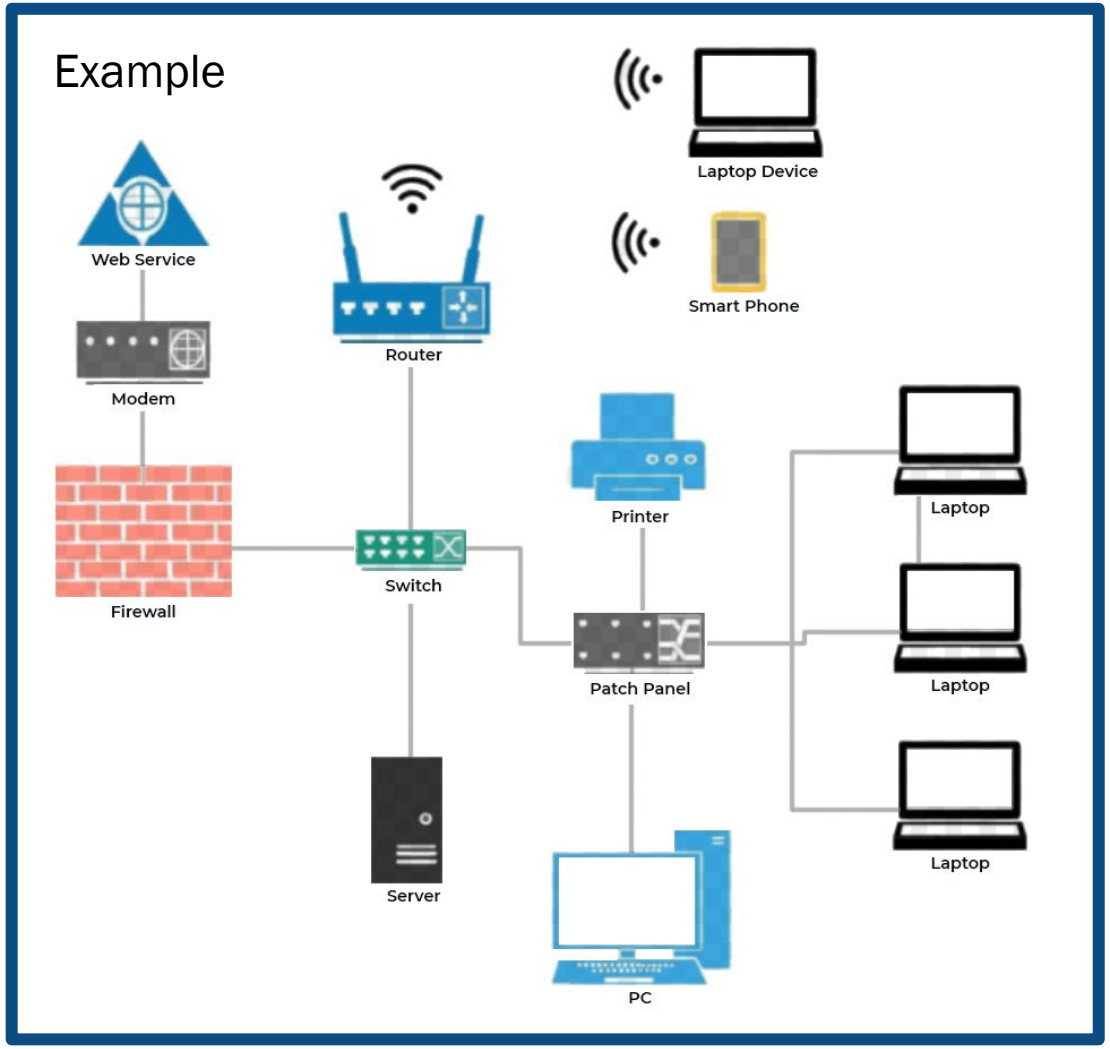
With your leadership team, including your lawyer

- Draw out your Information System
- Trace the flow of all information through that system
  - Intellectual Property
  - Financial Information
  - DoD Controlled Unclassified Information
  - HIPPA or PII
  - ITAR restrictions
- Understand the FARs, DFARS, CUI and your responsibilities

Draw your IS

Find some icons online and create a comprehensive drawing

Perhaps use a color on the components which handle CUI and IP, another color for FCI and another yet for PII



AFWERX SBIR ★ STTR

Corporate Decisions: What do you want?

- Do you want to simply comply with the law?
- Do you want to protect your entire company and all its data?
- Do you want to be able to do all business on your phones?
- What level of risk do you want to accept for your data and Information System?
- Do you realize that you need objective professional cybersecurity advice?

Telephone Example

- You've got to decide how you will use business telephones
  - Before you can purchase telephones and telephone security software/apps
- You've got to purchase telephones and telephone security software/apps
  - Before you can write policies and procedures on how to use them
- You've got to write policies and procedures on how to use them
  - Before you can provide training on the policies and procedures
- You've got to provide training on the policies and procedures
  - Before you give someone a business telephone

Your Options for an Information System Owner

- Assign someone the additional-duty of cybersecurity
- Hire a professional* 10-20 hours a week to run your cybersecurity program
  - These folks can use the open-source software and save you money.
    - NIST MEPs can work with your cyber pro to design very low-cost solutions
- Hire a managed service provider
- Hire a full-time cybersecurity professional
  - These folks can use the open-source software and save you money.
    - NIST MEPs can work with your cyber pro to design very low-cost solutions
- Other

Really, it is a business decision like any other

- Does this provider understand and respect your business model
- Are they qualified to give you advice?
- What is the implementation model?
  - What is the priority? The answer should be the 42, high-risk NIST SP 800-171 security requirements.
- What is the sustainment model?
- What are they going to do if you get hacked? (What are you going to do if you get hacked?)
- What are they going to do when you get audited? (What are you going to do if you get audited?)
- How are they going to hand the on-premise activities that need to be accomplished
- Talk to their customers, multiple customers to get a comprehensive picture of what is being offered.
- What is their own cybersecurity posture? Have they been hacked? Who protects the provider?

Who is Qualified to provide cybersecurity?

If you hire a consultant or 10-hour a week professional or other non-full time equivalent

- They should be certified. Professional certification, such as CISSP, CISA or CEH, show they are cybersecurity professionals. Be aware that some cybersecurity certifications are entry-level certifications, such as Security+, CSX, MTA
- They should have implemented NIST SP 800-171 in other businesses. They should have NO questions about what it takes to implement each of the 110 NIST SP 800-171 security controls, which have been the law for five years.
  - I talk to businesses each week who say their consultant has questions about NIST SP 800-171 – I say, “You hired the wrong consultant.”
- It’s going to cost you $200-$300 an hour if they are at the professional level to actually implement NIST SP 800-171. The pace is what you can afford.

What the provider should ask you…

- What are your plans to expand your business?
- What is your Information System inventory?
- What is your information System schema?
- What are your Information System goals?
- What types of data do you have?
- What is the data flow through your Information Systems?
- Who will implement solutions?
- Who will monitor your system?

What the you should ask the service provider…

- What are your certifications?
- What is your experience implementing NIST SP 800-171 in other small businesses my size
- What are your ties to cybersecurity vendors?
- What is your business model?
- How will we measure your progress?
- How will you test the cybersecurity you implement for my business?
- What is your availability/proposed schedule to implement NIST SP 800-171 for my business?
- What is your plan for sustainment of the IS security protections you implement for my business?
- Do you agree that we should first implement the requirements in FAR 252.204-21?

Your Managed Service Provider

- Service Level Agreement which provides you with SERVICE at intervals you need.
- Compliance documentation. When you tell the auditor you use XYZ-High, you still need to show every tiny detail of how that service meets one of the 110 NIST SP 800-171 requirements. Buckets of Documentation – on your schedule.
- Regular patch management
- End-to-end encryption.
- An Identity and Access Management capability that allows you to control access to your data- assign and remove administrative rights from users as needed.
- Endpoint platform protection(your printers, etc.)

Your Managed Service Provider

- An MSP with robust cyber protection combats the latest attack, like fileless malware and memory injections, with defenses that utilize cutting-edge technologies like machine learning.
- FedRAMP Moderate or Equivalent: FedRAMP moderate cloud offerings will be seen on the FedRAMP marketplace.
- New Attack Profiles: Fileless malware , Memory injections, Anti-malware solutions, Ransomware Protection, Anti-Spam Controls
- How do you log monitoring activities? logs that document the way they respond to your systems, networks, and devices.
  - Therefore, you should be able to request logs that capture activities on endpoints, routers, application events, proxies, and Internet-of-Things (IoT) devices.
  - Regular, routine backup and recovery

Your Service Level Agreement should contain…

- Overall strategy around cloud purchases/non-cloud purchases and integrating what you already have
- A Roadmap to full implementation
- Priorities
- A service-level agreement which meets your needs: daily, for audits, for emergencies, for buckets of documentation
- An understanding of who can see and manipulate your data
- An understanding of how the items they don't do – will be implemented.

Who will do What?

Here is an example of a MSP responsibility chart.
Who will do the items not in orange? Who will watch the MSP?

Always have a Roles and Responsibilities Chart for all 110 NIST SP-800-171 requirements.

For each of the 110 requirements and for other aspects of your Information System, understand and document:

- Who has Responsibility and skill to ensure each requirement is met sustainability,
- Who is Accountable for the success of your Information System and makes decisions
- Who is the subject-matter-expert on your team who must be Consulted on changes, and
- Who must be kept Informed on changes/incidents?

3.7.1	Perform maintenance on organizational systems.	Supports Compliance **Except** you must maintain your own infrastrucure maintenance (for onPrem solutions), policies, procedures and technologies
3.7.2	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Supports Compliance **Except** you must maintain your own infrastrucure maintenance (for onPrem solutions), policies, procedures and technologies
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	**Your Business' Responsibliltiy**
3.7.6	Supervise the maintenance activities of personnel without required access authorization.	**Your Business' Responsibliltiy**
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	**Shared Responsibility**

Artifacts of Compliance

- For each of the 110 security requirements you will need documentation, including screen shots, procedures, policies, etc. to prove to an assessor that you have achieved the standard is NIST SP 800-171A and a repeatable process for maintaining all 110 security requirements.

Laundry List of Artifacts which are meant to give you ideas of what kind of Objective Proof you can supply on each of the 110 requirements

- Documented policies, standards & procedures
- Supporting documentation to demonstrate how (software, hardware, etc.) is properly & securely implemented
- Screen shot of everything that could provide objective proof
- Documents or screenshot which demonstrate a capability
- Documents or screenshot to show how software or hardware are properly and securely configured
- Screen Shots groups and membership assignment
- Documentation to demonstrate change management practices reviewed/approved
- Data Flow Diagram (DFD)
- Screen shot of firewall rules with business justification
- Documentation of role-based security training being performed
- Screen shot of access control settings
- Screen shot of AD settings, or other IAM interface

MSSP Alert℠

Search for...

Our Newsletters: Subscribe Now

https://www.msspalert.com/

by Joe Panettieri • Oct 28, 2021

This blog offers an ongoing list of managed security services provider (MSSP) mergers and acquisitions that we've tracked.

At least five factors are driving the M&A activity, MSSP Alert believes.

1. **Talent**: The cyber skills shortage is driving MSSPs to find talent through M&A.
2. **Threats**: The growing, shifting threat landscape is inspiring M&A deals to close technology and expertise gaps.
3. **Speed to Market:** Acquiring companies can often be a faster path into a new or evolving technology market or business region.
4. **Scale**: Smaller MSSPs are merging to counter the scale of larger rivals.
5. **Growth:** The traditional MSP market will experience sub-10 percent compound annual growth rates (CAGR) in the years ahead. The MSSP market, in stark contrast, is growing at an 18 percent CAGR.

Updates: *This story was originally published May 7, 2019. It is updated regularly to reflect the latest MSSP-related M&A deals.*

Red Flags

- Any action which does not prioritize implementation of NIST SP 800-171
  - Which is CMMC Levels 1 and 2…
- Taking action on CMMC Level 3 before it passes through federal rule-making.
- Not talking with regard to full-implementation of security controls
  - We see many cybersecurity providers who want to provide you with a gap analysis and a list of things to do – but do not provide implementation.
- Handing you a set of documentation templates
- Not providing full-documentation on how their services and the software/hardware they sell you fulfill each of the 110 requirements of NIST SP 800-171
  - Cybersecurity is a culture, but you do have the task of showing documentation of compliance on 110 separate requirements
  - Some of the 110 will always be the responsibility of your business leadership - but there still needs to be a plan for the entire 110 requirements

Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to Kelley.Kiernan@us.af.mil
  - Daily Office Hours for answering/researching **your** questions about DAF Small Business cybersecurity and data protection!
  - **Every Tuesday**, 1pm Eastern, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar: https://www.zoomgov.com/webinar/register/WN_6Gz84TQGRvm6YHMSVyE0Qg