DIB MSP SHOPPING GUIDE FOR SMALL & MEDIUM-SIZED BUSINESSES

DECEMBER 6, 2022

Principal Authors:
Allison Giddens, Terry Hebert, Andy Sauer

DISCLAIMER

This content is developed by Member Company participants of the National Defense Information Sharing & Analysis Center (ND-ISAC) to assist and inform small and medium-sized businesses (SMBs) in selecting a Managed Service Provider (MSP) which can assist SMB compliance with evolving Department of Defense (DoD) cybersecurity requirements. This content is provided at no cost and is based on good faith analyses of best practices in consultation with external resources. Any actions or implementations based on this content are entirely at the user's risk and with no implied warranty or guarantee, or liability accruing to ND-ISAC or Member Company participants. This report may be excerpted or referenced but should not be appended or incorporated in whole within other products without the prior coordination of ND-ISAC (please contact: Info@ndisac.org); or, in any case, monetized for any purpose. **About the ND-ISAC**: ND-ISAC is a non-profit, non-federal entity established and funded by its member companies to support their collective cybersecurity and resilience against all hazards through multiple lines of effort (e.g. secure cyber threat sharing, technical solution working groups, knowledge exchange events). To learn more contact Info@ndisac.org.

THIS REPRESENTS THE FINAL REPORT & SUPERCEDES ALL PREVIOUS VERSIONS OR WORK PRODUCTS CREATED BY THE ND-ISAC SMB WORKING GROUP

It can be daunting for a small or medium-sized business (SMB) to know the right questions to ask a potential managed services provider (MSP), as the SMB – also an organization seeking compliance (OSC) – evolves in the Cybersecurity Maturity Model Certification (CMMC) space.

In a team effort, SMBs across industries[1] created this document to address the challenges presented to a SMB when vetting a MSP.

It is important to note that this document is to be used as guidance and considerations as you, the SMB, tackle the key premise: **Where is your data, who has access, and how is it managed, tracked, and protected?**

This document is intended to be approachable and meaningful for a SMB. It is organized in sections, with the first five questions helping to level-set the conversations. If a SMB finds that a potential MSP is not able to answer the first set of questions, in the interest of both time and mitigating risk, a SMB may likely choose to move on to another MSP.

Each question provides some context and recommendations.

Likely, most MSPs have not been asked all of these questions before now. Most questions are not intended to disqualify MSPs, but instead, intended to shed light on risks that exist that the OSC should consider when transferring cybersecurity responsibilities to a third party.

A secondary purpose of this guide is for MSPs to understand what risk concerns a SMB may have, and this could help the MSP improve upon their services to help in overall mitigation of risk.

The MSPs should be provided the questions [only], and then the SMB should use this full document to understand context and recommendations. A list of the questions are found at the end of this document for ease of copying/pasting to share with the MSP without the additional context and recommendations for SMB review.

A SMB may find it helpful to share these questions only with the MSP before a discussion or interview.

Remember: This document doesn't capture *all* scenarios. This is intended as basic guidance to help a business conduct due diligence in choosing an MSP/MSSP (both referred to as MSP in this document) that is well-suited to the environment in which the customer operates.

The SMB representative involved in this MSP conversation should include someone who understands the current cybersecurity posture of their organization, contractual requirements, and the business needs. This may be more than one person. It is encouraged to engage senior leadership early on, assuming they are not already filling one of the roles above.

---

[1] This document was created within the ND-ISAC SMB working group in collaboration with outside sources. Members of the working group attended different engagements and sought feedback from other SMBs across industries and the opinions of MSPs at their various engagements. All feedback was reviewed and used to create this living document. The goal will be to continually receive feedback and adjust the document on an as needed basis.

Table of Contents

Questions Only (for MSP use)

BASIC INTRODUCTION QUESTIONS

1. **Are you familiar with the National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" (NIST 800-171), Defense Federal Acquisition Regulation Supplement DFARS 252-204-7012, "Safeguarding covered defense information and cyber incident reporting" (DFARS 7012), and Cybersecurity Maturity Model Certification (CMMC)?**

    a. **Are you capable (and willing) to accept and implement DFARS-7012 flowdown?**

    b. **Do you intend on becoming CMMC Certified? If so, what level?**

    CONTEXT: *It's important to identify a Managed Service Provider (MSP) who is familiar with these basic standards in industry.*

    DFARS-7012 requires compliance around incident reporting, retaining data, etc. It's important for an MSP to not only be familiar with these requirements but confirm that they can comply with these requirements.

    RECOMMENDATION: A Managed Service Provider (MSP) should be familiar with these standards.

    You may find an MSP who is not familiar, or "getting up to speed" on these terms, but it is in your best interest to identify partners who have experience in this space.

2. **To which security framework do you align? Examples: National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), NIST 800-171/CMMC, State Requirements, Personal Identifiable Information (PII), Center for Internet Security standards (CIS), etc.**

    CONTEXT: *This will give you a broad sense of the vendor's security maturity.*

    RECOMMENDATION: An MSP should be able to provide a certification if they claim to be certified.

    The customer may request to see a vendor's Systems Security Plan (SSP). The vendor may not share the file or may offer restricted access. If the vendor denies access to their SSP, that is a business decision on whether to accept that vendor decision.

3. **Do you have a Customer Responsibility Matrix (CRM)?**

    CONTEXT: *A CRM is a document that formalizes what responsibilities are the vendors' responsibilities, and what are the customers' responsibilities.*

    The document should explicitly state the services being provided.

A clear delineation of responsibilities is important in day-to-day activities and assessments.

RECOMMENDATION: A Managed Service Provider (MSP) should be willing to develop one with you if they don't already have one available.

A business may opt to allow a Statement of Work (SOW) to serve as an acceptable alternative.

4. Are all people working for your company U.S. Persons?

a. Do you have anyone working abroad?

CONTEXT: *Many regulations, standards, and frameworks require information to be located within the U.S., staffed by U.S. persons, for example, ITAR and Export Control (more information here).*

If the vendor employs foreign nationals but can identify and assign only U.S. Persons to work on the customer's account, there should be something stated in a contract that mandates this requirement.

RECOMMENDATION: There is additional risk to consider if data is the vendor employs foreign nationals. It is highly recommended to consider only U.S.-based companies and persons who may have access to customer data – even inadvertently or unintentionally.

Additionally, from a business operation perspective, there is generally a higher level of support expected from U.S.-based companies.

5. If any of my data is stored on your information systems, where are those systems geolocated?

a. What of the company's data would you be storing? Examples: Controlled Unclassified Information (CUI), Controlled Technical Information (CTI), data applicable to International Traffic in Arms Regulations (ITAR), proprietary data, log data, etc.

b. If any export-controlled data is on customer's systems, is the data only accessible by MSP personnel who are U.S. persons?

c. If you start using offshore resources or are bought out by a company that does, will you give me advance notice and permit me to get out of the contract?

CONTEXT: *Many regulations, standards, and frameworks require information to be located within the U.S., staffed by U.S. persons.*

Depending on customer requirements, there may be limitations or restrictions on accessibility and privacy of data. If offshore resources are involved and not restricted by customer contract, it may be a business decision to work with the MSP.

RECOMMENDATION: There is additional risk to consider if data is scored outside of the U.S. It is highly recommended to consider only U.S.-based companies and persons who may access, store, and transmit customer's data.

If data is being stored in the vendor's cloud, they may be required to be approved within the The Federal Risk and Authorization Management Program (FedRAMP). Visit the FedRAMP Marketplace here for more information.

If the answer to "c" is "yes," ensure that this is explicitly called out in your contract. Work with the MSP to determine a minimum amount of time if necessary.

BASIC RISK MANAGEMENT

6. Where does my data exist in your environment?

a. Is my data separated from others' data?

b. If an MSP manages backups, what do those details look like? How are backups protected against destruction by ransomware or destructive malware? (e.g. immutability, offline, etc.)

c. What tools exist for copying data? Who has access? Is this audited?

d. If an MSP goes out of business, what happens to the customer's data?

CONTEXT: In many of the relevant frameworks, it is vital to minimize (if not eliminate) the risk associated with important data. If a company is relying on an MSP to maintain its data in the MSP's environment, there are several qualifying questions that should be asked to appropriately assess that risk.

*It is important to minimize the risk of incidental data access. (i.e., giving one customer access to view **their** data in the system should not give them access to view other customers' data in the system.)*

RECOMMENDATION: a.) Data should be logically segregated (i.e., customer information can be in the same system, but have different access controls).

In general, MSPs should not maintain and store customers' files. They should maintain data relevant data to manage services, but unless the customer specifies otherwise, the MSP should not retain the customer data.
MSPs should be able to identify specific data sets such as metadata, computers and information systems that they would regularly maintain, depending on the contract services.

b.) Data backups are an exception to the recommendation above. Data backups must have strict security access. MSPs should have explicitly limited access to customer backups.

c.) MSPs should be able to list systems that can copy data from a customer's system. An MSP should be able to list who has access and how this is audited.

d.) Depending on the MSP's role in maintaining and storing customer data, and your level of risk-severity, an escrow-service may be valuable to investigate.

7. What is your data retention policy?

a. Consider other industry requirements when this is answered, such as log retention requirements. Examples: ISO 9001 or AS9100 (Quality Management System Standards), Federal Aviation Administration standards (FAA), etc.

b. If you have log data, can you support our DFARS requirements?

c. How is my data destroyed when required? (secure deletion, for example)

CONTEXT: A customer may have contractual obligations to retain data for a specific length of time following the completion of a contract. Log data, metadata, data backups, and computer performance metrics may be part of those contractual requirements.

RECOMMENDATION: Throughout this document, when an MSP policy is referenced, it is recommended that the SMB ask to see the MSP's policy. If an MSP will not or cannot share (even via screenshare to limit distribution), this may be a red flag to the SMB.

A customer should review their contracts and know what they are required to do and communicate that clearly as flow-down to their MSP.

If there is no policy in place, a year is typically the standard length of retention.

8. Is multifactor authentication (MFA) enforced for administrator access? For Remote Access? For applications?

CONTEXT: MFA is one of the simplest ways of minimizing the risk of unauthorized use of accounts.

RECOMMENDATION: This is an absolute. There is no compromise. When your data is in question, the vendor *must* enforce MFA.

9. How does your team access my environment?

a. Do you use shared account(s)? Do you audit who uses the shared account(s)?

b. Do you use named accounts, assigned to individuals?

c. Do you use a break glass account?

d. Do you use just-in-time (JIT) access?

CONTEXT: It's important to understand how the MSP accesses their customers environments. Accountability and traceability are important – you need to be able to trace who – including MSP staff – does what in an environment. Just-in-time access is temporarily used by MSP staff when administrative access is needed.

RECOMMENDATION: a.) Ensure, when possible, the accounts with administrator access are not shared.

b.) Named accounts help ensure accountability and traceability.

c.) If MFA is not required on a break glass account, consider implementing compensating controls – there should be an alert when these accounts are used.

d.) The use of just-in-time access is the sign of a mature MSP.

10. Do you outsource anything to subcontractors?

a. Can you provide me with a organizational chart, and include any subcontractors if applicable?

CONTEXT: (Refer to questions 4-5) If a vendor does use subcontractors, it may be appropriate to ask in what roles. It is important for a business to determine if requirements should flow down to the MSP, and thus, its subcontractors if they use them.

If the roles are unrelated to the scope of work, the risk may be low to the customer.

RECOMMENDATION: Depending on the level of access to the customer's environment that the subcontractor has, it may be prudent to request (or require) a Customer Responsibility Matrix of the subcontractor via the MSP.

11. Do you have a Security Operation Center (SOC) or Security Information and Event Management (SIEM)?

a. Where do you receive cybersecurity threat briefings and who is part of the team that receives and analyzes them?

CONTEXT: A SOC is a function of an MSP that allows the MSP to focus on security issues from an organizational and technical level. A SOC monitors, detects, analyzes, and responds to cybersecurity incidents. An OSC should work with their MSP/SOC on any systems that transmit, store, or process CUI or systems that provide security functions.

A SIEM helps an organization recognize potential security vulnerabilities and threats before they become a problem.

RECOMMENDATION: The MSP should have a SOC or interface with a SOC (U.S.-based) that can meet requirements.

The SOC should have known threat sources and provide updated threat briefings on a regularly-defined basis.

An MSP may not internally manage a SIEM, so it's recommended that an OSC understand how an MSP meets the required objectives and maintains visibility (including normalizing/standardizing timestamps, which is vital for logging).

12. What internal governing policies does the MSP have in place? (examples - background checks, retention policies).

a. Do you have a policy stack that my company may incorporate/adopt, proven to be compliant with applicable framework or certification?

CONTEXT: If an organization does not already have documented policies in place, it may be efficient to adopt an MSP's policy stack after a thorough review to ensure there are no conflicting active business policies.

RECOMMENDATION: A mature MSP should have, at a minimum, high level guiding policies for cybersecurity. Ideally, they have specific policies they could share with the OSC. Some common policies or documentation to be considered: A Customer Responsibility Matrix, an Incident Response Policy and Hiring/Termination Policies.

13. What risk assessment are you performing on tools that you add to your environment that support my organization?

a. Do you have a Software Bill of Materials (SBOM) or full list of customer-facing stack?

b. How does your team mitigate the risk of attackers using MSP tools to deliver malware?

CONTEXT: Just as a customer should perform a risk assessment on their MSP, an MSP should be vetting the services it consumes, as well.

SBOMs are a relatively new concept, and while most MSPs may not have a SBOM, a very mature MSP may have one.

RECOMMENDATION: An MSP should evaluate their tools prior to implementation. They should regularly scan their tools for vulnerabilities. MSPs should also have valid and current vendor documentation for security on those tools. MSPs should be able to comprehensively address attackers using MSP tools.

14. How do you manage our passwords?

a. **Can you audit who has accessed them?**

b. **What are your requirements?**

c. **Do you use common passwords?**

d. **Do you reuse the same password across multiple systems?**

CONTEXT: MSPs generally store passwords in a system accessible to its staff.

RECOMMENDATION: An MSP should be able to audit who among their staff access customer passwords. They must not be using common passwords, and they should not be reusing the same password across multiple systems.

15. Do you perform Incident Response support for our systems?

a. **What are the response times (during business hours and outside)?**

b. **How often is the plan tested?**

c. **Can you support reporting requirements?**

CONTEXT: It is important to be on the same page with an MSP regarding the Incident Response Plan prior to an incident occurring.

RECOMMENDATION: If incident reporting as it relates to incidents in the OSC's systems is part of the scope of work, it's important for both the OSC and MSP to understand their roles.

A conversation should take place on the details of the IRP once an MSP and OSC agree to work together. All parties should be familiar with the sequence of events should there be an incident on the customer's systems that the MSP manages.

16. What is your company's (the MSP)'s Incident Response Plan (IRP)?

a. **How often is the plan tested?**

b. **How do you communicate with customers if their systems have been affected?**

c. **Can you support reporting requirements?**

d. **In the past 12 months, have you had an unplanned disruption to the services related to this scope of work?**

CONTEXT: It is important to be on the same page with an MSP regarding the Incident Response Plan prior to an incident occurring.

There may be publically-known compromises (Solarwinds, e.g.) and an OSC's leadership team may wish to confirm if wider issues affect their systems.

RECOMMENDATION: Request a detailed service-level agreement (SLA) if incident response is part of the scope of work the SMB intends to outsource to the MSP. Discuss what constitutes an incident and how the MSP will respond.

If incident reporting as it relates to incidents in the MSP's systems is part of the scope of work, it's important for both the OSC and MSP to understand their roles.

There may be parts to the MSP's IRP that are irrelevant to the OSC, but those conversations may take place if part of the CRM.

Additionally, an organization may wish to ask an MSP about its business continuity plans. The depth of these conversations depend on the scope of work and level of risk in question.

17. Can you expand on your hiring and termination practices?

a. **Do you do background checks on employees that have access to my data/account?**

b. **Are you willing to show your hiring/termination policy and checklist so I can ensure your people can be trusted to access my data?**

c. **Will you notify me immediately upon an employee being hired/terminated that has access to my data/account?**

CONTEXT: A customer should have control over who has access to their environment. Depending on data type (ITAR, for example), there may be a subset of MSP employees unauthorized to have access to customer data.

RECOMMENDATION: It is not recommended for a customer to micromanage an MSP's hiring and firing policies. This question and guidance exist more to prompt conversation between the customer and MSP, to understand typical data categories that the customer may own, and the requirements that the MSP frames for employment.

18. Can you tell me about your ideal client?

CONTEXT: As evidenced in many industries, if a company has many long-term customers, that is often a good sign. However, this may be tough to gauge if the company is young.

RECOMMENDATION: Ask for 3-5 references that are representative of your company's industry, size, and requested scope of work, if possible. Have open conversations with the references and ask questions like:

"How long have you been with the MSP?"
"Are you happy with the current service?"
"Are you satisfied with the response time of non-urgent and urgent requests?"
"Would you recommend them?"

19. Will you share your SSP with me?

a. Do you have a Supplier Performance Risk System (SPRS) score uploaded into the Procurement Integrated Enterprise Environment (PIEE)? Would you share a screenshot of your SPRS score with me?

CONTEXT: It is helpful to see how an MSP frames their network and manages their system. Much of the information on the SSP may give you some insight into other questions on this guide. When it comes to a company's SPRS score, it may be less about the actual score that's important, and more about the fact that they have one uploaded – if they say they have one uploaded. That said, the score may be very important if you are transferring risk to the MSP based on controls where they are lacking.

RECOMMENDATION: If an MSP will not share their SSP with you, ask why. They may be unwilling to share electronically but may be willing to host a virtual meeting and share a screen, or, if they are local and have a physical site, they may allow you to view a hard copy.

20. Are you a reseller of services, or provide direct?

CONTEXT: Just as a customer should perform a risk assessment on their MSP, an MSP should be vetting the services it consumes, as well.

RECOMMENDATION: There is no inherent problem with reselling services, as long the MSP has a good working relationship with the provider/source and has enough visibility into the system to assume risk.

INSURANCE

21. Do you carry cyber insurance?

a. Are you willing to add me to your insurance policy as an interested party?

b. What are your insurance limits?

c. Do you carry third-party cyber-insurance?

CONTEXT: Cyber insurance is becoming more common – and more expensive – over time. Many underwriters require a series of questionnaires. It helps to limit your risk exposure if your MSP maintains good cyber insurance coverage.

RECOMMENDATION: It is highly recommended that you read your cyber insurance policy questionnaire carefully and ensure that you are following the requirements to be insured. If you answer in the affirmative that you are following requirements, and an incident occurs, if it is later determined that you lied on your questionnaire, insurance will not cover the incident.

a.) An MSP should not have an issue adding a customer to their policy as an interested party. This is a relatively simple exercise that their insurance company can complete.

b.) Cyber liability coverage limits range between $500,000 and $5 million per occurrence, but once a claim is made, it is unlikely a company can be insured again, and if they can be, the premium is not insignificant.

c.) In the event that one of the MSP's subcontractors or outsourced service providers has an incident, and that incident affects your ability to provide product or service to *your* customer, you will be covered.

CERTIFICATIONS/COMPLIANCE

22. [If supplying hardware/network infrastructure] Is the product Federal Information Processing Standard (FIPS) Validated?

CONTEXT: FIPS validated encryption meets a specific set of requirements that protects cryptographic modules from being compromised or tampered with.

RECOMMENDATION: You can confirm that a vendor is FIPS 140-2 validated by searching on the NIST website. If the vendor is listed on the NIST website (here), it is reasonable to trust the vendor's technology.

23. Is company familiar (and compliant) with NDAA Rule Section 889, the National Defense Authorization Act for Fiscal Year 2020 (NDAA 2020) and the prohibited vendor list?

CONTEXT: DoD, GSA, and NASA included this provision in 2020 to prohibit the sale of and use of certain telecommunications and video surveillance services and equipment.

The U.S. Government piecemealed recent telecommunication and video surveillance services and equipment requirements.

RECOMMENDATION: A customer – and MSP, if they answer in the affirmative – should be very familiar and understand NDAA Rule Section 889 here.

At a minimum, the MSP (and SMB) should avoid the use of Huawei Technologies Co. LTD and Zhongxing Telecommunications Equipment Corporation (ZTE Corporation).

If an MSP cannot guarantee the avoidance of use of these companies' hardware, it is recommended that the SMB consult with an attorney.

24. Has your company undergone any audits or assessments, and what was the result? (ISO 27001, SOC 2, DIBCAC, etc.)

a. [if applicable] Do you have a Facility Security Clearance (FCL)?

CONTEXT: Depending on the services within the scope of work, it is a good sign if the MSP has successfully navigated key audits in industry.

RECOMMENDATION: At the time this document was written, inheritance is not something a business can take advantage of in the NIST 800-171 or CMMC space. However, if an MSP has had its system and environment vetted by successfully earning relevant certifications, that may help a business accept the lower risk in some areas of support.

Be wary of pay-to-play certificates and badges when they are used to support legitimacy in the market. Where certificates are not earned through assessment or audit and vetted by accredited bodies or industry-accepted means, take them with a grain of salt.

BUSINESS HISTORY

25. How long have you been in business?

CONTEXT: A business that has an established record is less likely to go out of business in the short-term. Of course, there are other factors that play into a business' viability in staying in business, but in today's IT-market, there are a lot of "fly-by-night" and MSPs that have popped up, claiming to have experience and knowledge in the space.

RECOMMENDATION: While there is no set number of years that a company *should* be in business, consider the length of time they have been in business as you weigh the overall risk of doing business with them, as you would any supplier.

26. Can you share references?

a. What is the average size business you serve?

b. Can you share a reference with a business that your incident response was tested?

CONTEXT: Just like any big purchase decision, a company should find out from others who are already doing business with the potential MSP, information beyond what an

MSP shares. Of course, the references are chosen by the MSP, so theoretically, the references would provide positive feedback about the MSP. It's still important, though, to have the opportunity to ask some candid questions: "How often do you find that you are using their tech support services?" "How long does it take for them to answer a typical support ticket?" "Do you work with one person primarily, or a team?"

RECOMMENDATION: It is recommended to talk to at least 2 references. Write out your questions in advance and gather as much information as you can.

Consider business size and industry, to compare apples to apples.

27. Is MSP's Data Universal Numbering System (DUNS) number or Unique Entity Identifier (UEI) on DnB or SAM.gov?

CONTEXT: A DUNS number means that a business has been validated by Dun & Bradstreet, a universal standard for tracking businesses and their financial transactions. In early 2022, the U.S. Federal Government transitioned from the use of DUNS numbers to the use of Unique Entity ID (UEI) numbers. In order to do business with the Federal Government, a company must have a UEI.

RECOMMENDATION: While an MSP may not need to apply for federal awards or contracts, they may not believe they need to register with SAM.gov. Depending on their role in handing data and being responsible for DFARS flow-down, it's recommended that the MSP be registered on SAM.gov.

28. Have you changed ownership or management in the last 12 months?

CONTEXT: The change of ownership or management is not necessarily a bad thing – but it may give you some perspective on the internal challenges that a business is facing. Additionally, finding out of they have been acquired or purchased is important. With ownership change may come internal policy change, which could affect the answers to the other questions in this survey.

RECOMMENDATION: It is important for an MSP to be as transparent as possible with you, the customer. While they may not be at liberty to discuss a pending sale of the business, if you commit to a contract to use their services, you may want to ensure that if significant changes in service or security come with the merger/acquisition, that you are given a pre- agreed-upon length of time to transition from the MSP, if necessary.

Questions only – for MSP use

BASIC INTRODUCTION QUESTIONS

1. **Are you familiar with NIST 800-171, DFARS 7012, and CMMC?**
    a. **Are you capable (and willing) to accept and implement DFARS-7012 flowdown?**
    b. **Do you intend on becoming CMMC Certified? If so, what level?**

2. **To which security framework do you align? (NIST CSF, NIST 800-171/CMMC, State Requirements, PII, CIS, etc.)**

3. **Do you have a Customer Responsibility Matrix (CRM)?**

4. **Are all people working for your company U.S. Persons?**
    a. **Do you have anyone working abroad?**

5. **If any of my data is stored on your information systems, where are those systems geolocated?**
    a. **What of the company's data would you be storing? (controlled information data, CUI, ITAR, proprietary data, log data, etc.)**
    b. **If any export-controlled data is on customer's systems, is the data only accessible by MSP personnel who are U.S. persons?**
    c. **If you start using offshore resources or are bought out by a company that does, will you give me advance notice and permit me to get out of the contract?**

BASIC RISK MANAGEMENT

6. **Where does my data exist in your environment?**
    a. **Is my data separated from others' data?**
    b. **If an MSP manages backups, what do those details look like? How are backups protected against destruction by ransomware or destructive malware? (e.g. immutability, offline, etc.)**
    c. **What tools exist for copying data? Who has access? Is this audited?**
    d. **If an MSP goes out of business, what happens to the customer's data?**

7. **What is your data retention policy?**
    a. **Consider other industry requirements when this is answered (AS9100/ISO, FAA, etc.), such as log retention requirements.**
    b. **If you have log data, can you support our DFARS requirements?**
    c. **How is my data destroyed when required? (secure deletion, for example)**

8. **Is MFA enforced for administrator access? For Remote Access? For applications?**

9. **How does your team access my environment?**
    a. **Do you use shared account(s)? Do you audit who uses the shared account(s)?**
    b. **Do you use named accounts, assigned to individuals?**
    c. **Do you use a break glass account?**
    d. **Do you use just-in-time (JIT) access?**

10. **Do you outsource anything to subcontractors?**

a. **Can you provide me with a organizational chart, and include any subcontractors if applicable?**

11. **Do you have a Security Operation Center (SOC) or Security Information and Event Management (SIEM)?**
    a. **Where do you receive cybersecurity threat briefings and who is part of the team that receives and analyzes them?**

12. **What internal governing policies does the MSP have in place? (examples - background checks, retention policies).**
    a. **Do you have a policy stack that my company may incorporate/adopt, proven to be compliant with applicable framework or certification?**

13. **What risk assessment are you performing on tools that you add to your environment that support my organization?**
    a. **Do you have a Software Bill of Materials (SBOM)?**
    b. **How does your team mitigate the risk of attackers using MSP tools to deliver malware?**

14. **How do you manage our passwords?**
    a. **Can you audit who has accessed them?**
    b. **What are your requirements?**
    c. **Do you use common passwords?**
    d. **Do you reuse the same password across multiple systems?**

15. **Do you perform Incident Response support for our systems?**
    a. **What are the response times (during business hours and outside)?**
    b. **How often is the plan tested?**
    c. **Can you support reporting requirements?**

16. **What is your company's (the MSP)'s Incident Response Plan?**
    a. **How often is the plan tested?**
    b. **How do you communicate with customers if their systems have been affected?**
    c. **Can you support reporting requirements?**
    d. **In the past 12 months, have you had an unplanned disruption to the services related to this scope of work?**

17. **Can you expand on your hiring and termination practices?**
    a. **Do you do background checks on employees that have access to my data/account?**
    b. **Are you willing to show your hiring/termination policy and checklist so I can ensure your people can be trusted to access my data?**
    c. **Will you notify me immediately upon an employee being hired/terminated that has access to my data/account?**

18. **Can you tell me about your ideal client?**

19. **Will you share your SSP with me?**
    a. **Do you have an SPRS score uploaded into PIEE? Would you share a screenshot of your SPRS score with me?**

20. **Are you a reseller of services, or provide direct?**

INSURANCE

21. **Do you carry cyber insurance?**
    a. **Are you willing to add me to your insurance policy as an interested party?**
    b. **What are your insurance limits?**
    c. **Do you carry third-party cyber-insurance?**

CERTIFICATIONS/COMPLIANCE

22. **[If supplying hardware/network infrastructure] Is the product FIPS-Validated?**

23. **Is company familiar (and compliant) with FAR Rule Section 889, the National Defense Authorization Act for Fiscal Year 2020 (NDAA 2020) and the prohibited vendor list?**

24. **Has your company undergone any audits or assessments, and what was the result? (ISO 27001, SOC 2, DIBCAC, etc.)**
    a. **[if applicable] Do you have a Facility Security Clearance (FCL)?**

BUSINESS HISTORY

25. **How long have you been in business?**

26. **Can you share references?**

    a. **What is the average size business you serve?**

    b. **Can you share a reference with a business that your incident response was tested?**

27. **Is MSP DUNS number (or UEI) on DnB or SAM.gov?**

28. **Have you changed ownership or management in the last 12 months?**