National Defense-ISAC

Securing Small Business Manufacturing Supply Chain Resource Handbook

March 2025

Tailored for the build-to-print defense contractor environment with use cases relevant to forging houses, manufacturers, and the finishing supply chain

ND-ISAC
National Defense Information Sharing and Analysis Center

EXECUTIVE SUMMARY

The National Defense Information Sharing and Analysis Center™ (ND-ISAC™) Small & Medium Business (SMB) Working Group is focused on sharing best practices to overcome resource-constraint challenges that many SMBs face. There are a variety of resources available to support small business cybersecurity implementation. For example, there is U.S. Government-funded research that explores challenges and solutions among small Defense Industrial Base (DIB) software development firms and white papers that offer SMB methods to engineer network segmentation. However, there are limited resources developed by DIB small business manufacturers that document common challenges for small businesses. This product illustrates real-world scenarios **in the build-to-print defense contractor environment with use cases relevant to forging houses, manufacturers, and the finishing supply chain**. As part of this the document amplifies specific and common challenges, and describes the risks that impact both the small business and the larger supply chain.

This product was developed for two primary groups of stakeholders:

1. **U.S. Government Personnel and large Prime Contractors** -- to explain common scenarios these stakeholders may not be aware of that impact security guidelines and requirements.
2. **Small businesses operating in the manufacturing supply chain** -- to offer practical steps both in immediate actions and long-term strategic planning to secure data and minimize risk.

The ND-ISAC SMB Working Group believes that broadened understanding of these challenges will enable more effective solutions.

Principal authors: Allison Giddens and Terry Hebert; with contributions from Ashton Momot, Vijaya Ramamurthi, and Andy Sauer.

DISCLAIMER

TABLE OF CONTENTS

INTRODUCTION

The scenarios and "notional" businesses described in this document are based on real-life circumstances shared among peers. Company names and selected underlying details were changed to protect the privacy of companies and individuals.

Many decisions made by small organizations are based on daily assessments about staying above minimum thresholds required to function as a business while simultaneously working to identify the primary risks associated with maintaining operations. Once a business has identified and is aware of a risk, it can address the risk. The decision could be to reduce (or mitigate) the risk - *expertise or resources permitting* - or to accept the risk as-is.

Risks identified in these scenarios are risks to the notional businesses in question but can also implicate the wider supply chain.

Suggestions made in this document do not take a single cybersecurity framework or regulation into consideration. Notes and observations made are general in nature, but based on the SMB Work Group's good faith analyses of best practices, informed by ND-ISAC member company subject matter experts who collaborate across a range of cybersecurity technical issues.

1.1 SUPPLY CHAIN & RELATIONSHIP DIAGRAM

It is important to track the flow of data **in a build-to-print defense contractor environment**. In a manufacturer's environment, the data that ends up in its environment typically starts with a U.S. Government request for quote (RFQ/RFP) made either to the SMB directly, or to a Prime contractor, and then flowed to the small business. The SMB translates the details into a deliverable and the product is shipped to a location per contract or purchase order. Activities in between the data entering a SMB manufacturing environment and the product arriving on the customer's dock carry many risks that should be identified and mitigated.

As is illustrated below in Figure 1, this supply chain typically starts from the U.S. Government communicating a need (or requirement) to its Prime (often the Design Authority) and then the Prime farms out components to assemble the final product along with any other deliverables (such as software or communications equipment[1]).

Not all steps are necessary to every project, program, or contract in the Defense Industrial Base (DIB) **build-to-print manufacturing environment**.

[1] While critical to the DIB, technology and communications equipment and their related supply chain issues are mentioned only briefly to maintain focus on the manufacturing supply chain.

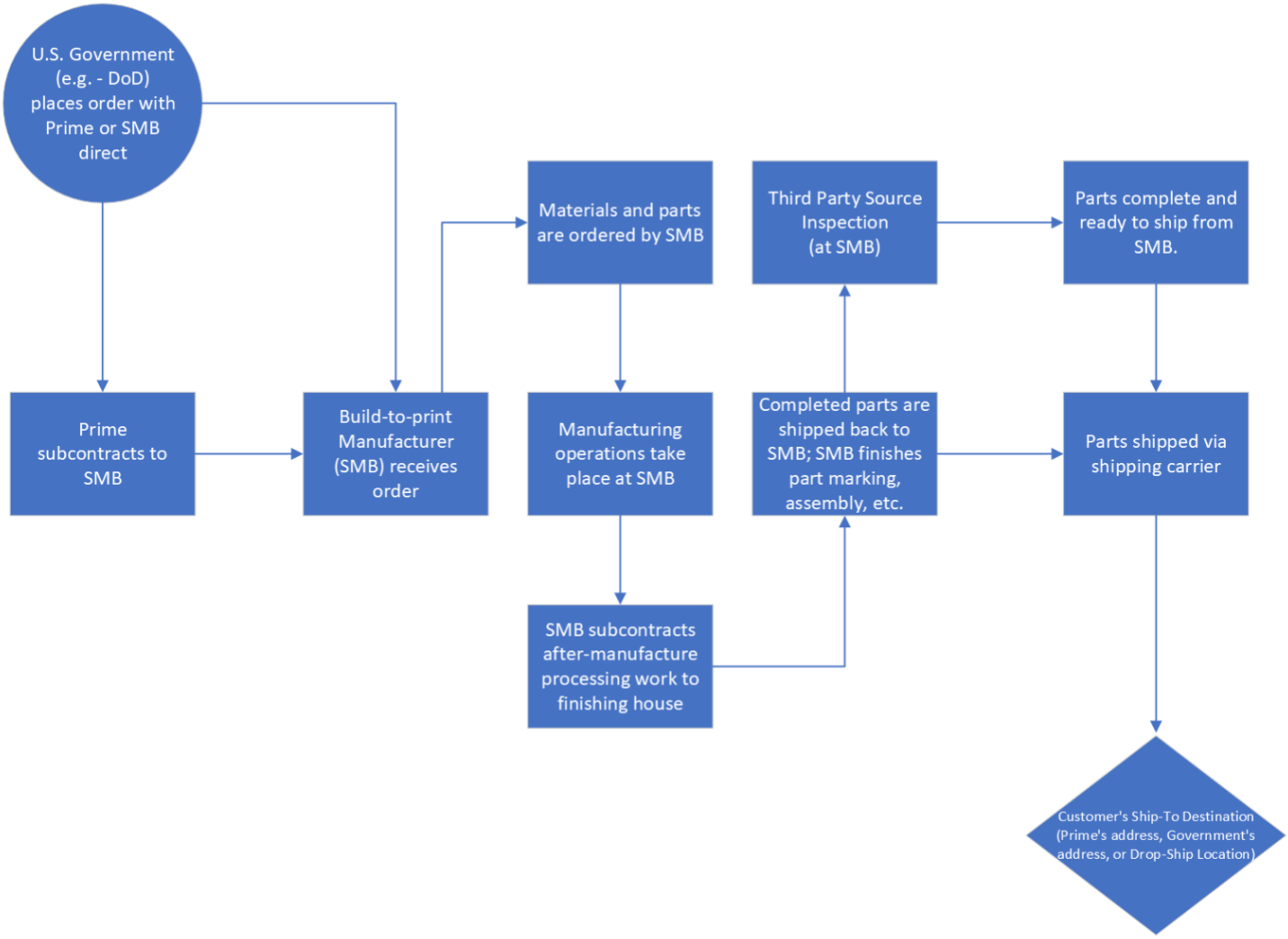

Figure 1: DIB Manufacturing Supply Chain Flow Chart

SCENARIOS AND BEST PRACTICE SUGGESTIONS

2.1 SCENARIO - UNNECESSARY ADMINISTRATIVE ACCESS

Situation: Gordan Tool & Die (GTD) is a third-generation machine shop. Started in 1940 by Joe's grandfather, the small shop employs 25 production workers and 3 office staff. For years, they have supplied tooling and fixtures to a large Prime that just happens to be down the street from GTD's 15,000 square foot warehouse. GTD operates off a single on-premises file server, which

contains thousands of designs for upper-level assemblies and flight hardware that the Prime has sent to them over the years. No doubt, GTD has much more data sent to them than they need to manufacture the parts. Oftentimes, that's helpful because it is hard to tell what features affect fit, form, and function without seeing an upper-level assembly. The three office staff personnel print the drawings for the production workers when they're needed.

What's the problem? (& risk): The office staff all have network administrative accounts which grants them administrative access to the server. If one of their accounts is compromised, the server (and all the data on it) is at higher risk of being corrupted, stolen or destroyed. Without the user's knowledge, any malicious activity could quickly spread to other systems. This could allow a malicious actor, whether a criminal or foreign adversary, to move around GTD's network freely. This lateral movement by the bad guy could bring the entire business operation to a standstill. The risk of using an administrative account even when administrative functions are not needed also enables a potential insider threat. An insider threat is not necessarily someone consciously acting maliciously – an insider threat can simply be an action that compromises the business from the inside.

What to do about it:

Now: Joe should immediately ensure the office staffers remove administrative access from their daily work accounts. Separate accounts should be created for the one or two people in charge of IT to use only when needed for administrative and privileged tasks – such as when software updates are to be installed, access policies are to be managed, patching or backing up data. Joe should also educate those in charge of IT to use administrative accounts only to complete these tasks. Likewise, those handling the IT chores should create and use separate accounts without administrative rights for email and other office tasks.

Soon: Office staff at GTD should ensure that the file server is backed up regularly, and the backups should be tested by restoring random files periodically. This way, in the event there is a server hardware failure or a cybersecurity incident, GTD will trust that the business-critical data can be restored. If possible, the backup should be maintained offsite (or uploaded to a cloud service) and regularly tested.

Why mitigating this risk matters to the supply chain: If GTD makes products that another manufacturer, the Prime, or the U.S. Government relies upon, an Information System or network disruption at GTD could cause ripple effects along the supply chain. This is because a company like GTD, or one that's been around a while, may unintentionally be a sole source for tools or equipment. Even if the tool is minor in the wider picture of a particular defense program, a disruption at GTD could produce broader secondary effects. The Prime would likely only identify a second manufacturing source if GTD was unable to bid on a part. This circumstance may create an array of adverse impacts for the contract or project that needs the tool.

2.2 SCENARIO - OUTDATED OPERATING SYSTEMS

Situation: Danny's Machining & Fabrication, Inc. (DMF) is a small manufacturer that has a range of capabilities such 5-axis milling, as well as waterjet and welding departments. DMF is a small one-stop-shop that larger companies come to for the manufacture of many sub-assemblies that support the F-35 JSF.

Workstations send programs to the shop machines using a variety of protocols such as ethernet and RS232 cables. The waterjet machine is connected to a Windows XP workstation on the company network. Jennifer is DMF's Office Manager, and she handles IT with the support of an outsourced managed service provider (MSP). Jennifer recognizes that the Windows XP workstation is old and needs to be replaced. She found a great deal at a big box retailer, and the new workstation comes with Windows 11 pre-installed.

DMF's MSP called the waterjet machine manufacturer to confirm that the new workstation had the right specs to run the waterjet's software. Unfortunately, the manufacturer of the machine gave the MSP some bad news: the controller on the $300,000 waterjet machine will not communicate with any operating system newer than Windows XP. The MSP broke the bad news to Jennifer: until DMF replaced the $300,000 waterjet, DMF would have to use a Windows XP workstation.

What's the problem? (& risk): Microsoft no longer supports Windows XP (and Windows 7, for that matter) with security patches. This means that over time, the lack of security and improvement updates will make DMF's aging Windows XP system vulnerable to criminal and foreign adversaries using newer threats and attacks that could compromise DMF's entire network. A workstation using unsupported or end-of-life software is more likely to be compromised through a vulnerability that would otherwise be patched on newer software. Additionally, there is a greater risk of a criminal or foreign adversary gaining access through it and moving to other devices in the company's network. Visit the Microsoft page on Product & Services Lifecycle Information.

What to do about it:

Now: Ideally, DMF should remove the end-of-life workstation from the company network. Even if data on this workstation is not sensitive or critical, this weak point in DMF's network introduces unnecessary risk. Alternatively, DMF may consider another method to transfer data to this workstation after disconnecting it from the network (such as a USB thumb drive), although removable media presents different security challenges (*see Scenario 2.3 below*). DMF should also contact the vendor of the waterjet machine and determine the correct version of the Windows Operating System that DMF will need to ensure its functionality after an upgrade.

Soon: While it is unrealistic to assume that DMF or other small manufacturer or fabricator has the resources to replace working machines simply because of security issues with a single workstation, it is reasonable to expect a small business owner to mitigate the risk they have identified. In this regard, DMF should inventory all other machines and equipment to determine if there are other systems that may have similar risk. DMF will want to analyze what it may take to budget for a replacement. DMF, in consultation with its supporting MSP, should also research what types of ways DMF can layer or segment the company network to prevent free movement if a bad guy gained access to the network.

Why mitigating this risk matters to the supply chain: DMF's range of capabilities means it is self-sustaining in many aspects of manufacturing that many of its competitors outsource. For example, DMF's waterjet can prep material stock quickly, allowing for machining operations to run more efficiently. Other companies may, by contrast, count on ordering material differently, or even drop-shipping material to be prepped before entering its machining environment. However, if DMF's waterjet is out of commission, and the company heavily relies on it to prep material stock, this could significantly delay the shipment of product. If DMF's customer is relying on the product for a larger assembly or program, this could impact delivery schedules all the way up the supply chain.

2.3 SCENARIO - USB FLASH DRIVES

Situation: Acme Assemblers is a small machine shop that specializes in aluminum sub-assemblies for testing laboratories led by U.S. Government agencies. Acme employs 100 people, with 30 of those 100 employees working as programmers and machinists on the shop floor who use any one of 15 workstations. Acme's work process calls for a programmer to log on to a shared Windows account assigned to their pod of engineers, create a program, and then save the file on a USB thumb drive. A machinist takes the USB thumb drive to a CNC machine, plugs it in, and saves the program to the computer interface, and runs parts at the machine. Occasionally, the machinist will tweak the program at the machine, re-save the file to the USB thumb drive, and put the drive back in any workstation to save the revised program to the company file server.

What's the problem? (& risk): The use of shared accounts can not only make it difficult to determine where a threat originated, but the lack of access controls for company workstations and unrestricted access to USB ports poses considerable risk of introducing malware on Acme's network and potentially disrupting the company's production processes. Unfortunate real-world experience confirms scenarios where a curious employee finds a stray USB flash drive in the company's parking lot or receives a USB drive at a conference and plugs it into a workstation at work to unknowingly introduce malware into the company's network. The malware in question could create an opening for a criminal or foreign adversary to surreptitiously search Acme's network, and steal files of interest or to hold Acme's network hostage with ransomware.

Additionally, if the stolen data is subject to U.S. Government controls (e.g. International Traffic in Arms Control Regulations (ITAR), Export Administration Regulations (EAR), DoD Controlled Unclassified Information (CUI)), Acme could be in violation of contract requirements or other jeopardy depending on the specific nature of the information controls.

What to do about it:

Now: The use of USB thumb drives is a vital expedient in Acme's business processes and removing USB thumb drives from the production floor overnight will cause serious business productivity harm. USB flash drives are often used on manufacturing shop floors to transfer data from workstations to CNC machines. In some cases, manufacturers choose to use RS232 cables or hardwire machines and operational technology (OT) in other ways. In cases where a shop floor uses USB flash drives, "allow-by-exception" policies can be set to effectively protect data and still allow for productivity. However, it's essential for Acme to immediately reduce the risk to the company by doing four things to prevent "rogue" removable media devices in Acme's production environment:

1. Block USB ports on workstations not essential to production and create an "allow-by-exception" policy to authorize the use of only specific, pre-approved USB thumb drives.
2. As a condition of approval, before first use, the USB thumb drives must be scanned for viruses or malware on a workstation with actively updated anti-virus software.
3. The scanned and pre-approved USB thumb drives should be used only on-site, used exclusively for production purposes, and be stored on site.
4. Maintain a log of the USB thumb drives to include check-in and check-out procedures.

Soon: Investigate potential options for individual user access to workstations such as personal login accounts or assign certain workstations to specific users and if possible, implement multifactor options such as a Yubikey. Also, consider safer portable drives such as company managed external drives with encryption. These types of business process changes can cost significant dollars and impact workflow. It is important to bring key individuals at the company into this conversation so options can be explored.

It is important to note that some drives formatting or encrypted drives may not work with older machines on a traditional shop floor. Before committing a lot of funds to a single solution, Acme should consider testing proposed solutions on the workstations and equipment (if applicable) before putting into production.

Why mitigating this risk matters to the supply chain: If Acme Assemblers' company network goes down, it will take time for Acme to get back up in operating mode which will impact other companies who were relying on Acme to supply product. Acme's ability to get back online and continue business operations will depend on their ability to respond to an incident quickly, with backup copies of their business critical data to aid restoral. A poor or delayed response could

significantly delay product to Acme's customer with adverse impact for a larger assembly or program and associated delivery schedules.

2.4 SCENARIO - PHISHING

Situation: Janet has worked for Aerospace Machining Metrics (AMM) for 20 years in accounts payable. She's part of a small front office and is tasked with matching up invoices to pack lists and certifications from the shop's suppliers. AAM's job shop has hundreds of suppliers: primarily aluminum suppliers, rivet distributors, and plating processing houses. Because the company is always making so many different new products it is always onboarding new suppliers. Janet has a hard time keeping up with so many new names. Recently, many more suppliers are opting to email invoices instead of mailing them to Janet through the U.S. Postal Service. Some suppliers send .pdf invoices through Quickbooks, some send documents as attachments, and some email Janet links to click on and retrieve the invoice. Janet often struggles to differentiate legitimate emails from phishing attempts (i.e. bogus emails pretending to be from a genuine supplier or individual intended to scam the receipient into revealing sensitive personal, financial, or network access information).

What's the problem? (& risk): Phishing is one of the most common attack methods used by cyber criminals. Some phishing attempts shrewdly include style, wording, and cues associated with authentic businesses. If Janet misses (sometimes subtle) errors in an email, all it takes is Janet clicking once on a link or opening a file attachment to install malware. If Janet has local administrative account access, this problem could be even bigger, leading to data compromise. (*see Scenario 2.1*)

What to do about it:

Now: AMM management should ensure Janet is not using an account with network administrative access when she is preforming her accounts payable duties. Additionally, AMM should provide Janet with phishing training to help her learn how to spot cues in potential phishing attempts and report them for defensive actions.

Depending on the email client and application that AMM uses, the IT department or AMM's MSP should use available security features to help filter legitimate emails from bad emails.

Soon: AMM should also identify others at the company who need similar training. Many companies have reported positive benefits by implementing a phish report initiative with incentive rewards for employees who report phishing emails.

Why mitigating this risk matters to the supply chain: AMM's employees are the company's first and last line of defense. AMM management will increase the probability of the employees

remaining vigilant by offering mandatory phishing training at regular intervals. If malware delivered by a phishing email takes down AMM's network, it not only affects the department's function (such as accounting) but it affects the entire company. As a second order impact, AMM's network outage would also affect those companies to whom it owes money – its suppliers. In turn, the combination of effects will probably impact the delivery of product that AMM committed to its customers. More broadly, a successful phishing attack can also trigger a cascading effect to other companies AMM does business with if malware delivered by a phishing email compromised an AMM employee's address book.

2.5 SCENARIO – SHARING SENSITIVE DATA 1

Situation: Main Street Manufacturing & More (MSMM) is a small business that specializes in precision machined parts. It does not work directly with the Department of Defense or other federal agency; it is a Tier 2 supplier (also known as a subcontractor) and works closely with several large Primes. MSMM makes complex parts and sends them to authorized-finishing houses (per the Prime's requirement) for anodizing, paint, and other plating requirements. MSMM's Prime customer has a list of approved processing houses that MSMM as a manufacturer can choose from. These processing houses have been vetted for quality by the Prime customer, but not for their cybersecurity posture.

When MSMM ships parts to an approved processing house for masking and anodizing, the processor requires a copy of the blueprint to be sent to them, since the drawing has specific information regarding the finishing and after-plating dimensions. The data is often not clearly marked with any type of data classification, and the tough-to-read blueprints are scanned pages from large plotters, with designs "proved out" in the 1970s.

Because of its work with the Prime, MSMM is assuming that the data, while unclassified, is sensitive. Because of this circumstance, MSMM knows they should not simply email the drawing to the processing house. Notwithstanding MSMM's reservations the only processing house authorized to process per the required specification claims that they "receive these types of prints via regular email all of the time."

What's the problem? (& risk): Mis-marked (or not marked at all) data is commonplace in a manufacturer's environment. MSMM also understands that Primes and government contracting officers are rarely *also* aerospace engineers, so their contracting staffs cannot be expected to fully understand what the manufacturer does and does not need to make the machined part.

Added to this, if the Prime requires MSMM to make a part that will go into a larger subassembly, and the data for the machined part appears on page 3 of a 12-page subassembly PDF print, the

Prime or government contracting officer will likely provide MSMM the full 12-page subassembly PDF print.

To complicate matters, MSMM may be asked to manufacture part number FJ987-**88**. However, the print may be named FJ987.pdf and the subassembly part number named FJ987-**1**. Further, there may be several other parts manufactured by several different machine shops, and all go into a completed FJ987-1 subassembly – and it is likely that they are all defined on the FJ987.pdf.

Irrespective of their place in the supply chain MSMM and its peers contend with a fact-of-life circumstance: it's easier for the Government or Primes' contracting staffs to provide the full 12-page print. As a practical circumstance to help reduce information superfluous to its production task MSMM does not have a full Adobe suite license to remove and reorganize the pages.

However, removing and reorganizing pages creates other potential issues. In doing so, MSMM may inadvertently discard pages and data that would assist MSMM (or its subcontractors) to make the part to specification. For example, based on experience MSMM knows that, oftentimes, the bill of materials and processing notes are found on the first page of the drawing package. If the part being manufactured has a key characteristic or feature that is important to the assembly, there may be additional information the MSMM needs elsewhere in the packet. As a result, for configuration management purposes, separating data may be more problematic to product quality. All things considered, MSMM does not necessarily consider receiving the 12-page PDF document as "overkill" for its needs.

However, here's the catch for MSMM: Depending on the Prime or federal agency's requirements that have been flowed down to MSMM by their Prime, MSMM is responsible for how – and to whom – they share this data.

To culminate MSMM's situation, when the only processing house on a short list of customer-approved processing houses asks MSMM to simply email the sensitive data package without using secure file share methods, the MSMM must consider its responsibilies as:

- A data steward, ensuring appropriate sharing and security of data;
- A manufacturer, seeking qualified subcontracting services to complete a conforming manufactured part, and
- A trusted supplier, meeting on-time deliveries with minimal disruption and grief back up the chain to its customer.

MSMM is concerned that it does not have the resources to perform a thorough risk assessment on its own supply chain. MSMM is limited in supplier choices and is driven by its Prime to use the Prime's supply base. Resource constraints are common throughout the entire supply chain and MSMM believes that it is not realistic to think their small company can manage other's

learning curves in security compliance, when they are barely able to devote time (and people) to keep up, themselves.

What to do about it:

Now: If the processing house cannot receive data in an encrypted form or through a secure file share platform MSMM should consider mailing a hard copy. If this is not feasible, and time is of the essence, it may be prudent to have a conversation with the Prime customer to identify another processing house.

Soon: MSMM should have a more detailed conversation with their processing house as to why they are unable to receive secure files. Are they sharing an email box that is preventing them from accessing a secure file share link? Are they admittedly not tech-savvy? MSMM may be in the position to provide some basic guidance. Or are the issues in question something that may require the assistance of the processor's IT staff or Managed Service Provider (MSP) -- if, indeed, the processor has one?

Why mitigating this risk matters to the supply chain: After-manufacture finishes are vital to aerospace and defense products – both in part integrity and product safety. In today's Defense Industrial Base small business manufacturing environment, Primes and Design Authorities identify approved suppliers that have been vetted in quality management systems such as ISO 9001, AS9100, NADCAP, and Prime-proprietary processes. Given these requirements it is not easy to become an approved processing house for a Prime or Design Authority[2] and, therefore, for MSMM and peers the list of customer-approved processing houses for specific specifications in defense programs is short.

This relatively limited universe of approved processors (aka finishing houses) for critical manufacturing processes such as cadmium plating, nickel plating, and other finishes, creates the potential for broader supply chain disruption. If one or two finishing houses are unable to meet cybersecurity requirements and therefore are unauthorized to receive data, this could hold up a products essential for national defense.

2.6 SCENARIO – SHARING SENSITIVE DATA 2

Situation: Main Street Manufacturing & More (MSMM) finally worked out their finishing house issue and securely sent the finishing house the data they needed to process the parts. MSMM's managed service provider (MSP) helped the finishing house IT Manager (who is also the

[2] A Design Authority is an engineer (often at the U.S. Government or Prime) that is responsible for establishing design and technical requirements of a product. A Design Authority is often the owner of the design.

company's Office and HR Manager), but after a lot of effort, they identified a solution that enabled them to securely share sensitive data.

Now, MSMM has a completed order of parts that require third party inspection. The inspector typically handles this by visiting the plant. But the inspector recently moved a few hours away and is still assigned to his old region until a local inspector can be assigned. As a work-around in lieu of traveling to MSMM's plant, the inspector says he requires a camera to be used for a live view of the parts.

MSMM has a company camera but it does not take video. MSMM does not use webcams and the only video cameras on-site are those on employee's cell phones, which are not allowed on the plant floor.

What's the problem? (& risk): MSMM does not have a bring your own device (BYOD) policy and does not provide guidance or assert any control over employee-owned devices as it pertains to their use for business purposes. MSMM worries that videoing potentially sensitive data and product on an uncontrolled device may be a problem per its Department of Defense related contracts and industry regulations.

What to do about it:

Now: MSMM should explain its concerns to the inspector and ask if he will accept photos uploaded via secure file share or would reconsider an in-person visit. This can be a tough conversation to have, as MSMM never wants to come across as a difficult supplier to an inspector!

Soon: If these types of instances are likely to occur more frequently MSMM should investigate investing in an inexpensive portable device (such as a tablet) managed by the company's security policies. Alternatively, MSMM might develop a bring-your-own-device (BYOD) policy; although managing a BYOD policy my pose its own issues for MSMM.

Why mitigating this risk matters to the supply chain: MSMM takes seriously its responsibilities to appropriately handle and secure defense information. Based on the request from the inspector, MSMM suspects the third-party inspector may be a contractor who may not be familiar with security requirements that are flowed down to the manufacturer. MSMM's experience suggests it is important to communicate concerns to inspectors. Across the defense industrial base, and depending on an inspector's tenure, they may be hyper-aware of these concerns and may be able to suggest appropriate workarounds they've seen used elsewhere. Because the inspector sees product at many different suppliers, the inspector may be able to offer insight into the creative ways that others have managed compliance (without breaching NDAs, of course).

2.7 SCENARIO – SHARING SENSITIVE DATA 3

Situation: Titan Edge Manufacturing (TEM) sent an aluminum part to FinishPro Coatings to be primed and painted. While the part was for one of TEM's aerospace customers, the print and data supplied was not marked with any caveat such as CUI, ITAR*, or any other type of categorization of sensitive data. Regardless, TEM sent the data encrypted when it emailed the file to FinishPro (as it is company policy to always send customer data encrypted, regardless of categorization). (*Controlled Unclassified Information or CUI, and International Traffic in Arms Regulations or ITAR)

After FinishPro shipped the painted part back to TEM, FinishPro emailed a .pdf file to TEM's purchasing agent. The first page of the .pdf file was a cover sheet displaying the caveats "****ATTENTION****" and "CUI – SENSITIVE."

The next page of the .pdf was a pack list for the part that had been painted and the third page was the standard, boilerplate certification for the paint job.

What's the problem? (& risk): There are several problems and risks associated with over-classification of data.

Mislabeling non-sensitive information as CUI can lead to unnecessary security precautions. This increases the cost and complexity of handling the information without justification. It can also cause unnecessary operational delays in processing or communication as stakeholders may hesitate to handle the information without additional security measures.

Additionally, frequent improvised markings can desensitize recipients to the importance of correctly labeled sensitive information, leading to potential mishandling of actual CUI in the future.

Contracts often define how CUI must be handled. FinishPro Coatings' labeling of the information as CUI could therefore be interpreted as a failure to understand or adhere to regulatory definitions of CUI. This could create audit risks or concerns during inspections by customers or regulatory bodies. Worst case, incorrectly marking data as CUI could lead to accusations of mishandling, even if no real sensitive information is involved.

Correspondingly, if TEM treats the mislabeled data as CUI, TEM might apply inappropriate handling protocols, further creating inefficiencies and complicating interactions with downstream suppliers or customers.

For TEM's aerospace customer, the mislabeling might reflect poorly on TEM's subcontractor, FinishPro, and by extension, on TEM itself. This could damage trust and raise concerns about both companies' ability to manage sensitive data.

What to do about it:

Now: The purchasing agent at TEM should call FinishPro Coatings and explain why the data should not have been marked sensitive or CUI.

After FinishPro Coatings understands that the data is not sensitive, FinishPro should resend the electronic shipping and certification .pdf package to TEM -- minus CUI markings.

Soon: This situation reveals a gap in FinishPro's understanding of CUI definitions and marking standards. Proper training is essential to ensure that employees know when and how to apply sensitive data classifications. Arguably, due to complexities in marking guidance, its unsurprising that CUI rules can be difficult to follow at times.

At a minimum, FinishPro should establish clear communication protocols with customers such as TEM to verify data classification and handling requirements. In circumstances where TEM is unable to answer FinishPro's questions about data supplied by TEM, TEM should reach out to *its* customer to resolve the issue.

Why mitigating this risk matters to the supply chain: Correctly identifying data is not just about meeting compliance requirements. Correctly identifying data has downstream effects on reputation and operational efficiency for all links in the supply chain. Data identification begins at the U.S. Government agency level and should be clearly communicated to its supply chain.

2.8 SCENARIO – PHYSICAL SECURITY

Situation: Quality Fab Leads (QFL) is a 50,000 square foot two-building facility that employs 190 employees. QFL has state-of-the-art machinery and equipment, including a large 3D printer. They have people coming and going constantly and run two shifts – a day shift and a night shift. Maintenance people, employees, local school tours – QFL may as well have a revolving door at the front lobby.

What's the problem? (& risk): Many security frameworks and industry standards require variations of access control. If QFL is not appropriately monitoring and tracking who is coming and going on-site, they are not securing company premises, equipment, or data, whether it's proprietary data or DoD controlled unclassified information received under contract.

What to do about it:

Now: QFL should institute access control procedures. As a minimum the company should require all visitors to stop at the front lobby and sign in before visiting anywhere on the property and wear visitor badges so employees are aware the visitor is allowed on site.

Soon: QFL should install a method to control access to doors such as keys, keyfobs or card readers at doors leading into the buildings. QFL should also require non-employees or personnel not previously vetted to be escorted by an authorized person at all times.

Why mitigating this risk matters to the supply chain: Physical security is an essential in companies within the Defense Industrial Base, whether as a proprietary interest, a contractual requirement, or to comply with DoD's evolving cybersecurity requirements. Depending on the nature of QFL defense work there may be specific contractual criteria which require specific physical security measures. While QFL has proudly opened its doors to school tours (to encourage future employees), QRF should evaluate whether the tours and related photography may pose a security concern to products based on DoD controlled unclassified information, or controlled under other requirements such as International Traffic in Arms Regulations (ITAR).

To a shop that proudly has its doors open to students in the community to encourage them to consider a career in manufacturing (a trade and industry that desperately needs growth), restricted access can often be a hard pill to swallow, prompting a company to think creatively to engage the next generation workforce.

2.9 SCENARIO – SHIPPING & LOGISTICS

Situation: Millathe, Inc. is a company that manufacturers large ground support equipment for the U.S. Air Force (USAF) through a couple of larger Primes. Sometimes, though, Millathe works with the USAF directly, other times through the Primes. When working directly with the USAF the company is instructed to identify a less-than-truckload (LTL) freight company. When working through the Primes the LTL freight company is chosen for them.

Millathe, Inc. purchases large lots of material from forging houses with mills located across the country, though Millathe prefers to do business with certain companies over others. Millathe is also affected by their suppliers' truck driver shortages and rising fuel costs, which the suppliers pass along to impact Millathe's bottom line. If that's not enough, in what seems like a regular occurrence, LTL freight companies are reporting cybersecurity incidents much more frequently than ever before. LTL freight companies are usually smaller companies (similar to the ones represented in these scenarios) who have a harder time recovering from cybersecurity incidents.

What's the problem? (& risk): These types of challenges may be somewhat peripheral to DoD or Prime contracting staffs but can exert significant adverse impacts to a small business, particularly when the small business relies on a single supplier (or transporter). If Millathe has agreements with a trucking company that experiences a cyber incident that disrupts the trucking company operations, the incident likewise disrupts Millathe's operations. Any material that is in transit to Millathe is at risk of delay and, correspondingly, any product that has yet to be picked up from Millathe is at risk of not meeting its delivery schedule to the customer.

What to do about it:

Now: Millathe should notify customers that Millathe is monitoring industry events and risks and will keep the customer in the loop on expected delays. Millathe should work with its insurance agent to not only purchase cyber insurance, but also to consider third-party cyber insurance, as well. Cyber insurance may be helpful if Millathe experiences a cyber incident, but third-party coverage goes one step beyond. Third-party cyber insurance ensures that if one of the Millathe's suppliers or transporters in Millathe's supply chain is impacted by a cyber incident, and this affect's Millathe's ability to sell product to their customer, Millathe will be covered under this policy.

Soon: Millathe should consider diversifying options for shipping. If one freight company is unavailable or begins to slip in communication or meeting due dates, Millathe should consider choosing another.

Why mitigating this risk matters to the supply chain: While this scenario does not weave specific technology or cybersecurity compliance into the challenge, logistics issues represent a serious ongoing business vulnerability for SMB, with potential impacts to Primes and programs. Well described supply chain disruptions triggered by the COVID-19 pandemic impacted a range of US industry sectors and production processes. However, small businesses seldom have the depth of resources that contribute to business resilience or have the leverage available to larger organizations to influence suppliers, vendors, or customers. For many small manufacturing businesses supply chain risks may be mitigated by diversifying sources of support and product. However, diversification presents a new set of risks, including more complex management and coordination, tasks, and expanded footprint of exposure, plus additional costs.

2.10 SCENARIO – HIRING

Situation: IronClad Solutions is an engineering firm in the Southeast U.S. that is desperate to grow its workforce. Last year, they doubled their revenue and demand for their services as a design and build-to-print shop has grown exponentially.

Alex Lee, a recent graduate from a local university, stopped by with his resume and eager to show IronClad what he could offer. He had taken classes in SolidWorks and seemed willing to work the night shift. He didn't have the experience IronClad really needed and Alex wasn't turnkey, but at least he knew his way around some of the machines.

Within the first couple of days of Alex's start date, Human Resources ran his social security number through eVerify and the system reflected a mismatch. The HR Manager had never seen this before and worried. Did this mean Alex shouldn't be on the floor at that very moment or handling sensitive data? The company was very short-staffed - were they going to be back to drawing board to fill this role?

What's the problem? (& risk): Employing someone who is not authorized to work in the U.S. is a violation of federal law and can result in fines and penalties. Allowing an unauthorized worker to handle sensitive data, particularly in a design and build-to-print shop that may involve proprietary or regulated information, could create compliance risks (e.g., export controls or ITAR).

What to do about it:

Now: An eVerify mismatch does not immediately disqualify someone from working. It indicates a need for further investigation. Common reasons for a mismatch include:

- A typographical error in the data entered (e.g., incorrect social security number or name spelling).
- An update or delay in government records (e.g., new naturalized citizens).
- Fraudulent documentation or intentional misrepresentation by the employee.

After the HR Manager confirms that it was not a typo by the company that caused the mismatch error, the company must notify Alex about the mismatch as soon as possible and provide him with an opportunity to resolve the issue. eVerify provides a "Notice of Tentative Nonconfirmation" (TNC) which should be shared with Alex which explains the mismatch and his right to contest it.

While Alex is allowed to continue working during the contest period, given the potential compliance risks, IronClad should assess whether he should handle sensitive or export-controlled data. In a small business like IronClad with considerable work in the aerospace

industry, it is not likely there is much Alex will be authorized to work with if he is not a U.S. Person.

Soon: Assuming that the reason for the mismatch was due to employee fraud (and not something such as a typo or issue on the government side), IronClad's desperation to grow its workforce may possibly have led to overlooking red flags during the hiring process. The company should balance its need for talent with thorough vetting to avoid compliance risks.

Why mitigating this risk matters to the supply chain:

Our adversaries know that the barriers to access a small business shop floor are weaker than a large corporation's. Small business resources are often spread thin across many departments. In fact, the US Government recognizes this is a key risk as one of the four long-term strategic priorities of the National Defense Industrial Strategy is Workforce Readiness.

In many cases, the business may not have a full-fledged "Human Resources Department," but rather, an Office Manager who also serves as the HR Manager. Consequently, interviewing, vetting, and on-boarding practices for a small business may not be as stringent as they are for larger businesses with the resources to support these efforts. In today's market where key industries face a growing demand for skilled labor, businesses may find themselves in a difficult position when the pool of qualified candidates authorized to work on US Government contract work is minimal.

Looking longer term IronClad would benefit and could participate in US Government programs focused on high demand career initiatives, apprenticeship programs, technical and trade schools, and re-skilling opportunities to grow the workforce in new and creative ways. This would support IronClad and other industries need to fill skilled trade worker vacancies.

2.11 SCENARIO – INCIDENT RESPONSE PLANNING & DOCUMENTATION

Situation: ForgeWorks Inc. is a small, family-run forging house in the Midwest that specializes in creating high-strength, precision components for industrial equipment manufacturers. The firm has grown steadily, securing contracts with larger companies in aerospace and automotive industries. Despite its success, ForgeWorks has not prioritized formalizing cybersecurity practices due to limited resources and a lack of perceived risk.

One morning, an employee in the engineering department at ForgeWorks opened an email attachment that appeared to be an email from the Human Resources Department. The text of the email included a link, with instructions to click the link to update the employee's direct deposit information. Unfortunately the attachment contained ransomware. Within minutes, key

files on the company's network were encrypted, and a message appeared which a Bitcoin payment in exchange for the decryption key.

The ransomware attack crippled ForgeWorks' operations: production schedules were inaccessible and customer order details were encrypted. ForgeWorks had no documented incident response plan (IRP) and no designated team or process to handle such an event.

Employees, including IT support staff, were unsure of their roles and responsibilities. Some attempted to troubleshoot the issue, while others called external IT service providers for help.

Without a formal plan, management decided to pay the ransom, fearing further delays in production and potential contract penalties. They wired the payment but never received the promised decryption key.

ForgeWorks delayed notifying customers about potential delays hoping to resolve the issue quickly. When word got out it strained relationships with key clients, some of whom were concerned about data breaches affecting their proprietary designs.

The ransomware incident also involved the encryption of personally identifiable information (PII) from employee records. ForgeWorks was unaware of its obligation to report this breach under applicable state and federal regulations, exposing the company to potential fines.

What's the problem? (& risk): The absence an incident response procedures or documented plan (IRP) has severe consequences:

If hit with a cyber incident, the absence of an IRP can extend a company's downtime – and adversely affect customers and suppliers that rely upon ForgeWorks goods and services.

An incident can generate significant costs to ForgeWorks: – a ransomware payment, external IT consultants for a cleanup, penalties from missed customer order deadlines, loss of future work, and government fines or regulatory penalties.

What to do about it:

Now: Caught flat-footed without an IRP means an improvisational trial and error approach to restoring the ForgeWorks network, and considerable probability of failure.

However, Immediately following the incident, the ForgeWorks team should sit down to talk through the incident and take notes about what happened along the way. This post-mortem may help in the development of an IRP for future purposes.

Soon: ForgeWorks should (a) invest in cybersecurity training for employees to prevent phishing attacks, (b) develop a robust backup system to ensure data could be restored without paying a

ransom, and (c) develop a documented IRP tailored to the company's risk profile. Additionally, ForgeWorks should test that IRP annually through a tabletop exercise to ensure when the need arises the ForgeWorks team is familiar with their respective roles.

Why mitigating this risk matters to the supply chain: Supply chain, delays or disruptions at one business can ripple through other businesses, leading to widespread operational and financial impacts. Many small businesses in the defense supply chain are now required to comply with cybersecurity frameworks like NIST 800-171 and soon, CMMC. An IRP is a fundamental part of these frameworks.

Finally, a documented IRP demonstrates to customers, prime contractors, and partners that the business is prepared to manage and mitigate risks, and therefore fosters trust and confidence. Beyond this, larger companies and U.S. Government cybersecurity contractual requirement ~~are~~ increasingly mandate an IRP.

2.12 SCENARIO – SNAKE OIL

Situation: BrightMetal Finishing, an aerospace finishing house, has been growing steadily and recently secured contracts with a Tier 1 aerospace supplier. These contracts require compliance with stringent cybersecurity regulations, including NIST 800-171 and the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC). BrightMetal Finishing hired an external Managed Service Provider (MSP), SecureSolutions Tech, to manage its IT and cybersecurity needs.

Initially, SecureSolutions Tech seemed like a perfect fit. They offered very affordable services and promised to handle BrightMetal's IT needs, including compliance. In fact, SecureSolutions Tech promised CMMC readiness in a matter of months! However, over a short time, BrightMetal began to encounter red flags:

- SecureSolutions Tech installed basic antivirus software and a firewall but did not implement multi-factor authentication (MFA), network segmentation, or endpoint detection and response (EDR) systems, all critical for compliance with aerospace cybersecurity standards.

- BrightMetal assumed the MSP understood the regulatory requirements, but SecureSolutions Tech had no experience with NIST 800-171, CMMC, or ITAR. Instead, SecureSolutions Tech provided generic IT solutions that did not address specific compliance controls.

- During a phishing attack, BrightMetal's network was partially compromised. When SecureSolutions Tech was contacted, they were unable to respond effectively, having no incident response plan or forensic capability.

- BrightMetal believed its network was monitored for vulnerabilities, but SecureSolutions Tech only ran occasional, superficial scans. When a third-party auditor assessed BrightMetal's readiness for CMMC, the third-party auditor identified multiple deficiencies, putting BrightMetal's Tier 1 contract at risk.

What's the problem? (& risk): BrightMetal is out of compliance with NIST 800-171, potentially violating contractual obligations and federal regulations. Noncompliance could lead to fines, contract cancellations, or loss of eligibility to work on DoD projects.

The phishing attack highlighted how ill-prepared BrightMetal and its MSP were to respond to incidents. Delays in resolving the issue affected production schedules.

Tier 1 aerospace suppliers rely on secure, compliant partners. BrightMetal's failure to meet standards could damage its reputation and result in losing future opportunities.

What to do about it:

Now: BrightMetal should conduct a thorough review of SecureSolutions Tech's performance and capabilities using a guide such as the ND-ISAC DIB MSP Shopping Guide for Small and Medium-Sized Businesses. If SecureSolutions Tech intends on continuing to support aerospace clients with DoD contracts but cannot achieve compliance with CMMC, with SecureSolutions support or by themselves, it may be time for BrightMetal to devise an exit strategy and transition to another MSP with validated experience in supporting regulatory compliance (e.g. DoD's CMMC based on NIST 800-171 controls).

Before investing in expensive tools to supplement support from a new MSP, BrightMetal should investigate no-cost offerings from the NSA Cybersecurity Collaboration Center and the DoD Cyber Crime Center (DC3) and its DoD Defense Industrial Base Cybersecurity Partnership. As part of this BrightMetal should implement multi-factor authentication (MFA) for all accounts and secure sensitive communications with encryption. BrightMetal should also work to segment the network to limit potential damage from any breaches.

Soon: BrightMetal should hire a cybersecurity auditor to assess gaps in compliance and security posture and use the audit findings to create a prioritized action plan.

Assuming a new MSP is onboarded, clear expectations should be defined for both the MSP and BrightMetal using a Shared Responsibility Matrix.

Why mitigating this risk matters to the supply chain: Weak security at BrightMetal creates a vulnerability in the wider aerospace supply chain. A data breach or cyberattack could expose sensitive data from other suppliers or prime contractors.

APPENDIX A - ACRONYM AND AGENCY GUIDE

CISA: Cybersecurity & Infrastructure Security Agency

CISA is a Federal agency. It "connects stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people."

CISA is an operational component of the Department of Homeland Security (DHS).

CISA org chart

FedVTE: Federal Virtual Training Environment

The Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and US military veterans.

FedVTE is a tool under CISA's umbrella.

NCSC: National Counterintelligence and Security Center

NCSC "leads and supports the U.S. Government's counterintelligence (CI) and security activities critical to protecting our nation; provide CI outreach to U.S. private sector entities at risk of foreign intelligence penetration; and issue public warnings regarding intelligence threats to the U.S."

NCSC professionals also serve as the Executive Staff for the Director of National Intelligence as Security Executive Agent (SecEA). Presidential Executive Order EO 13467, assigned the DNI responsibility for effective and uniform policies and procedures governing access to classified information for the Intelligence Community (IC) and government-wide.

The Office of the Director National Intelligence (ODI) has 4 centers under it: Counterterrorism, Counterproliferation, Counterinfluence, and CI & Security (the NCSC).

NCSC leadership

The Office of the Director National Intelligence (ODI)'s website
The Office of the Director National Intelligence (ODI)'s org chart

NIST: National Institute of Standards and Technology

NIST is one of the nation's oldest physical science laboratories. Its mission is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."

NIST is part of the U.S. Department of Commerce.

NIST org chart

The Government of the United States Org Chart

APPENDIX B – RESOURCE LIST OF TOPICAL GUIDES

This appendix is adapted from the "Securing Small and Medium-Sized Business Supply Chains: A resource handbook to reduce information and communication technology risks."[3]

Cyber Expertise: The availability of knowledge, skills, and experience necessary to establish, implement, and manage ICT SCRM practices. Collaborating is a key factor for a company to invest in cyber expertise most effectively.

Recommended mitigation resources for this risk category:
CISA: CISA Cyber Essentials
CISA: CISA Cyber Hygiene (Vulnerability Scanning Services)
CISA: Cyber Resilience Review Assessment
CISA: Cyber Security Evaluation Tool (CSET®)
NIST: Ransomware Resources
NIST: NIST Cybersecurity Framework (CSF) Quick Start Guide
NIST: Small Business Cybersecurity Corner (including Cybersecurity Case Study Series)
NSA: Govsheild DNS, Vulnerability Scanning, Threat Intel
DC3: DoD Cyber Crime Center and DoD DIB Cybersecurity (CS) Program

Executive Commitment: Executive commitment really means an energetic orientation among the company leaders and managers toward a range of factors: engaged company leadership, knowledge and understanding of cybersecurity as a business risk and a willingness to foster an organization-wide cyber risk awareness culture. The latter means prioritizing cybersecurity risks, mitigating them, and enabling secure supply chain practices necessary to protect the company, its assets, employees, and customers.

Recommended mitigation resources for this risk category:
CISA: CISA Cyber Essentials
CISA: Cyber Guidance for Small Businesses
DNI: Supply Chain Best Practices
NIST: Baldrige Cybersecurity Excellence Builder
NIST: NIST Small Business Cybersecurity Corner
NIST: Small Business Cybersecurity Community of Interest

Supply Chain Risk Management: Processes and practices ensuring the integrity of your supply chain aimed at improving a company's cybersecurity practices by identifying, assessing, and mitigating the risks associated with information technology products and services. This can include engaging relevant stakeholders, investing in the appropriate resources to protect the

[3] Link to CISA resource: https://www.cisa.gov/sites/default/files/publications/Securing-SMB-Supply-Chains_Resource-Handbook_508.pdf

company's data, and integrating cybersecurity practices into the company's decision making, budget, and operational processes.

Recommended mitigation resources for this risk category:

CISA: Internet of Things (IoT) Acquisition Guidance
CISA: Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium-Sized Businesses
CISA: Best Practices in Cyber Supply Chain Risk Management
CISA: CISA Cyber Essentials
CISA: Cyber Resilience Review Assessment
CISA: Cyber Security Evaluation Tool (CSET®)
CISA: Cybersecurity Incident and Vulnerability Response Playbooks
CISA: Mitigations and Hardening Guidance for MSPs and Small and Mid-sized Businesses
CISA: Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services
ENISA: Threat Landscape for Supply Chain Attacks — ENISA (europa.eu)
FEDVTE: Cyber Supply Chain Risk Management for the Public
NCSC: Framework for Assessing Risks
NCSC: Supply Chain Best Practices
NIST: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
NIST: Executive Order (EO) Guidance for Cybersecurity Supply Chain Risk Management
NIST: Manufacturing Extension Partnership (MEP) Resources
NIST: NIST Secure Engineering
NIST: NIST IR 8374 Ransomware Risk Management: A Cybersecurity Framework Profile | CSRC

REVISION CHANGE LOG

Revision 2

1. Minor grammar, spelling corrections
2. Minor clarifications made in existing scenarios
3. "What to do about it, now" expanded under 'USB flash drive' scenario
4. Added Scenario: "Sharing Sensitive Data 3" (now 2.7).
5. Added Scenario: "Hiring" (2.10).
6. Added Scenario: "Documentation" (2.11)
7. Added Scenario: "Snake Oil" (2.12)
8. Edited Appendix B to remove DC3 resources qualifier for cleared contractors only; updated links to Cybersecurity Incident and Vulnerability Response Playbooks and Cyber Supply Chain Risk Management for the Public.

To learn more about the National Defense ISAC go to: www.ndisac.org
Interested in joining our community? Contact info@ndisac.org