WHITEPAPER

The Total Cost of DoD Cybersecurity Compliance

NeoSystems®

TABLE OF CONTENTS

Executive Summary

Many companies will struggle to meet the cost and complexity associated with achieving Cybersecurity Maturity Model Certification (CMMC) compliance. CMMC introduces a rigorous and comprehensive set of cybersecurity standards, which may entail significant investment in technology, personnel, and processes. Additionally, the certification process involves audits by accredited third-party organizations, adding another layer of complexity. Transitioning existing systems and practices to align with CMMC requirements can be time-consuming and disruptive, calling for careful planning, training, and coordination across the organization.

We'll examine each of the top cost drivers that impact government contractors ability to achieve and maintain DFARS and CMMC compliance. Many of these have a greater impact on small and medium-sized government contractors because the solutions require economies of scale. Options may encompass buy versus build solutions, as well as enclaving.

TAKE-AWAY

Security cost drivers include the following:

- **Continuous Monitoring –** requires investment in technology and skilled personnel
- **Security Hardening –** requires developing, deploying, and maintaining a secure configuration baseline that still supports business operational requirements
- **Configuration Management –** tracking changes in systems is a step often neglected, but is required
- **Patching –** vulnerabilities are continually identified and need to be remediated
- **Encryption –** requires running in FIPS mode with FIPS validated cryptography
- **Multifactor Authentication –** supporting disparate MFA solutions required by different cloud services providers
- **Attack Detection –** requires the tools to detect and the human analysis skills to investigate which alerts represent unauthorized use or false positives
- **FedRAMP Cloud Services –** need to confirm that your SaaS solutions as well as the tools your MSP is using meet the requirements

Beyond Compliance

This paper also explores the challenges and ways to address (outdated) legacy systems and specialized assets, including manufacturing control systems as well as approaches to BYOD in a compliant system.

There are some common contractor mistakes that can drive up compliance costs including misinterpretation of controls, incomplete solutions, and overspending on assessment. One of the most common mistakes we see contractors make is the misinterpretation of controls.

A recurring theme in this paper is that the ongoing cost of maintaining effective security and compliance is the dominant financial factor. As contractors consider their security spending, they should seek accurate estimates of the ongoing monthly costs as well.

They might over-interpret the requirement and engage in "gold-plating" that goes above and beyond the necessary expense to meet the government's intent. An example is issuing duplicate end-user devices (e.g., phones, laptops) and then requiring workers to use separate devices for their government-related work and everyday corporate functions. One the other hand, the contractor might implement a solution that does not fully meet the requirements. In the worst-case scenario, the contractor might have to rip-and-replace their original solution with a compliant solution. An example is choosing a firewall or wireless router from a vendor that does not support FIPS-validated encryption.

Contractors all want to minimize their cost, but that doesn't mean they can accept shortcuts or inferior security. In choosing their partners, contractors should insist on service providers – both cloud services and managed services – that will contractually commit to compliance with the same standards and regulations the government is flowing down to the contractor.

A recurring theme in this paper is that the ongoing cost of maintaining effective security and compliance is the dominant financial factor. As contractors consider their security spending, they should seek accurate estimates of the ongoing monthly costs, whether that is cloud service subscriptions, managed service fees, or internal employee labor costs. We examine several requirements that are process-intensive: configuration and change management, continuous monitoring, patching, and detection. These are requirements that cannot effectively be met by set-and-forget methods. They are ongoing by nature. Any solution budget that does not explicitly include these functions should be questioned.

TAKE-AWAY

Retrofitting or adding security to existing systems sometimes proves to be the most expensive way to achieve compliance. Fortunately, contractors have options including:

- **Migrating** to a modern purpose-built IT architecture
- For businesses that can segregate people and/or data, **enclaving** can be a good way to limit compliance scope (and therefore cost)
- **Purchasing cloud services** can easily demonstrate compliance with the FedRAMP standards
- Implementing a **standardized solution** with minimal customization; this unlocks the economies of scale that come from re-use of proven solutions.
- **Integrating** IT, security, and compliance operational functions using a **"SecOps" approach**

Background

Companies that provide services to the federal government are obligated to comply with stringent cybersecurity compliance requirements. And not without good reason. Study after study has validated significant losses of government intellectual property and technological advantage due to cyber threats focused on commercial companies in the government supply chain. Of particular concern is the Defense Industrial Base (DIB). These 300,000+ companies work with information and technologies that are critical to our national security – information and technologies that are highly sought after by our adversaries.

The government's objective in imposing these compliance requirements is to make its supply chain more resilient – making it less susceptible to cyber-attacks. The government is using a number of regulatory levers to spur the private sector to improve the effectiveness of their defenses.

All involved – the government and its contractors – want to spend smartly on cyber defenses. Although the government is using regulations to set minimum compliance standards, it's up to contractors to determine the most cost-effective methods for meeting those standards. Often, cybersecurity costs – and benefits – are not obvious. While competing solutions might each meet the "letter of the law" with respect to compliance, they may vary widely in cost, convenience, and security effectiveness. Which solutions deliver the most "bang for the buck?" Which suffer from the "law of diminishing returns"? Which will most confidently demonstrate compliance? Which are considered controversial by authorities (or auditors)? Which will grow with our business? Which will prove unworkable in practice? By looking at the important factors that impact security spending decisions, company leaders can make informed decisions on these complex tradeoffs.

Compliance Regulations

Cybersecurity compliance regulations are not new. The Federal Acquisition Regulation (FAR) has imposed "basic safeguarding of covered contractor information systems" – fifteen security measures that apply to any systems with Federal Contract Information (FCI) – on essentially the entire government supply chain since 2016. The Defense Federal Acquisition Regulation Supplement (DFARS) added "safeguarding covered defense information and cyber incident reporting" requirements to contracts originally in 2013 and updated it to its current form (requiring implementation of NIST SP 800-171) with a "full security requirement implementation date" of December 31, 2017.

Over five years later, many contractors are still working to achieve full compliance. Assessments performed by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), as well as other studies, have found that a large percentage of defense contractors have not implemented all the required controls; many have barely started. The DoD has responded with a rulemaking effort to impose independent certification requirements via the CMMC initiative. While CMMC is

not a contractual obligation today, the rule making process to make it a contractual obligation is in process. DoD has stated their intention to make certification a prerequisite to receiving a DoD contract award, either as a prime contractor or subcontractor at any tier.

Contractor Challenges

After years of regulatory pressure, why do large gaps still exist? Cost is a major factor. Lack of expertise to interpret and apply complex security controls is another.

We have ample evidence that compliance – and security resilience – are inconsistent and generally inadequate across the contractor landscape. After years of regulatory pressure, why do large gaps still exist? Cost is a major factor. Lack of expertise to interpret and apply complex security controls is another.

As contractors set their IT and security budgets, the cost of compliance is often not clear. Companies often mis-judge the level of spending required to achieve and maintain compliance. The requirements, specifically the 110 controls specified in NIST SP 800-171, cover a wide range of technical, administrative, and physical controls. The government provides contractors with latitude in determining how to best meet the control objectives, and the security marketplace presents many options. It is not straightforward to assess the alternatives, nor to fully understand the total life-cycle costs of achieving and maintaining compliance.

As a service provider, NeoSystems has worked with hundreds of companies that need compliant IT solutions. Across all these companies, one common experience has been that it's not feasible to "add on" security to bring existing IT systems into compliance. Essentially all companies need some degree of IT transformation to achieve compliance with federal cybersecurity mandates. While "bolt-on" security is often the first path companies investigate, this approach falls short for both technical and administrative reasons.

On the technical side, the security hardening and approved cryptography needed to meet federal regulations is not the default for commercially available software. Special configuration steps must be taken, and generally these need to be done at the time the system is first built. Adding it onto existing systems is difficult or impossible, making it more cost-effective to move to new systems. Another technical factor is that some major vendors offering cloud-based office productivity software-as-a-service (e.g., email, collaboration, document management), including market leader Microsoft, have separate environments for customers that need federal compliance. Often this means companies must migrate from their existing commercial cloud service to a compliant government-oriented service.

On the administrative side, the government standards, specifically CMMC and the DIBCAC assessment practices, emphasize maturity: the degree to which security practices are institutionalized. The government standards cover many practices traditionally carried out by IT staff or Managed Service Providers, for example configuration management, system hardening, and software patching. In most cases, the tools and procedures used by the IT team need to be operated maturely. This means they must be well documented, followed closely, and produce

Essentially all companies need some degree of IT transformation to achieve compliance with federal cybersecurity mandates .

evidence of compliance on an ongoing basis. For most IT teams, this is a major overhaul of operating practices. And for Managed Service Providers, this requires a level of transparency that most cannot (or will not) accommodate. Similar to the situation with cloud service providers, many companies find that they need to migrate from commercially focused managed service providers to a vendor that is willing to sign up for the requirements imposed on government contractors.

It is well documented that there are not enough skilled cybersecurity practitioners to fill needed roles. This leaves the private sector competing for expertise. Small and medium sized businesses are at a disadvantage when it comes to attracting top cybersecurity talent, in large part because their needs may not be sufficient for individuals seeking full time indefinite employment. And also because security skillsets are highly specialized. A small security team may, by necessity, only consist of a few generalists, and be lacking in the specialized skills a larger team would include. A small team may struggle to perform all the needed security practices. While large companies can scale up their security team to include the needed skillsets, most small and mid-sized companies find it necessary to contract with one or more specialized security services firms to cover all the requirements.

These challenges add uncertainty to the budgeting process, in particular the risk of making wrong decisions or accepting bad advice. The marketplace for federally compliant IT services is still evolving, and it is difficult to be certain that a particular solution or service is going to be both functionally successful and compliant.

Life Cycle Cost Factors

Although it's tempting to view security compliance as a "project" or "initiative" in which we budget money to move from a non-compliant "before" state to a compliant "after" state, this viewpoint tends to under-represent the ongoing costs of maintaining compliance. Companies that focus on the up-front costs such as gap assessments and remediation/migration costs often are surprised by the "forever" cost to stay compliant after the "project" is completed. Or worse, they are unable to fund those costs and revert back into a non-compliant state, effectively wasting their up-front investments.

Tennis legend Arthur Ashe is quoted as saying "Success is a journey, not a destination. The doing is often more important than the outcome." Cybersecurity is much the same. Achieving compliance just long enough to pass an audit doesn't help much with the cyberattacks that come after. To stay safe, secure, and compliant, it's necessary, and required, that security practices be sustained, monitored, and adapted to ever-changing threats.

In the life-cycle diagram below, the left three phases, Assess, Select, and Configure, are often thought of in terms of one-time project costs. This includes planning and design work, technology and service acquisition, migration to new systems, and documentation of policies

and procedures. They may need to be revisited as technologies age out, but these are considered the up-front costs of becoming compliant.

The rightmost phase in the diagram, Manage, encompasses the ongoing costs to execute the required security practices. Particularly in the case of cloud services and managed services, there are often monthly subscription fees that extend for the life of the business. Maintenance, monitoring, and adaptation are other necessary activities that occur in this ongoing operations phase.

"Success is a journey, not a destination. The doing is often more important than the outcome."

To stay safe, secure, and compliant, it's required that security practices be sustained.

Cybersecurity Compliance Life Cycle

ASSESS

1. Determine scope, boundary, and CUI data flows for the CMMC environment
2. Evaluate corporate security policies
3. Evaluate IT use cases and current environment
4. Complete Security Control Matrix

SELECT

1. Select best-fit reference architecture
2. Identify any needed modifications
3. Set up prototype

CONFIGURE

1. Complete system security plan and supporting security program documentation
2. Complete production IT build-out
3. Migrate users and data
4. Train users

MANAGE

1. Continuous monitoring
2. Capacity/performance monitoring
3. Vulnerability/patch management
4. Chnage management
5. User support
6. Break-fix
7. Audit readiness/support
8. Security governance

The cybersecurity standards for federal contractors place a heavy emphasis on on-going protection activities. Set-and-forget strategies, even those based on sophisticated defensive technology, will not fully satisfy the government's compliance requirements. Nor will passive strategies adequately protect against determined attackers. The cyber threats we face are dynamic, and effective protection must include active components.

Although automation can go a long way in improving cyber defenses, the capital cost of devices such as firewalls and encrypted wireless access points are no longer the dominant cost in a cybersecurity budget. Two major sources of on-going cost must also be considered: software-as-a-service subscriptions and human operational costs.

Most security software vendors, and indeed most software vendors in general, have moved to a cloud-based software-as-a-service model where pricing is typically dollars per seat per month. In the security space, this shift recognizes that security defenses must be continually updated as threats and risks change. Key parts of the security stack are functionally superior when using a cloud model versus static software: anti-malware, intrusion prevention, identity and access management, mobile device management, and e-mail protection to name a few. The reason cloud approaches work better is that these security functions benefit from large-scale data aggregation and continual updating – two things that work very well in a cloud-based model.

There are several aspects of a compliant cybersecurity operation that are human driven. Although automated tools may support the human effort, there is still a need for an operations staff with diverse yet highly specialized skills. Functions such as security analytics, alert/incident response, risk management, and configuration management rely heavily on human attention and decision making. In considering the ongoing cost of these operational functions, companies must consider both the workload and the skillsets required. As noted earlier, we have a chronic shortage of cybersecurity skillsets. It's very easy for a small or mid-sized company to over-task their security team. Typically, these teams are small and not able to handle the surge of work that might come during a security incident, for example. Also, being small, they may be unprepared to perform functions that are outside their skillset. Either of these "over-tasking" scenarios can lead to security and compliance failures. For most small and mid-sized businesses, the security operational function should be performed by, or augmented by, a specialized managed security service provider (MSSP). The MSSP model provides the elasticity to handle the natural ebbs and flows in security effort. And MSSPs typically have larger teams – spread over many clients – to allow them to tick all the skill boxes with true specialists.

Top Cost Drivers

The government's cybersecurity mandates for contractors revolve around the NIST SP 800-171 standard: "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." As the title indicates, this standard is focused on Controlled Unclassified Information (CUI). The term CUI encompasses a very broad range of data, with 125 categories of CUI covering defense, financial, law enforcement, nuclear, legal, privacy, and other types of data. Contractors that handle CUI need to protect it in accordance with the NIST SP 800-171 standard. The government will typically impose this standard as a contractual requirement in any contracts where the contractor could receive or create CUI as part of their performance of the contract. This is the baseline minimum protection for CUI. Certain types of CUI may have specific safeguarding requirements that are above and beyond this baseline, and these will be specified in the contract.

The top cost-affecting controls examined here are:

1. Continuous Monitoring
2. Security Hardening – Least Functionality
3. Security Hardening – Nonessential Functionality
4. System Baselining
5. Security Configuration Enforcement
6. System Change Management
7. Vulnerability Remediation
8. Data in Transit and Data at Rest
9. CUI Encryption
10. FIPS-validated Encryption

Other important factors:

- Multifactor Authentication
- Identify Unauthorized Use

For contractors that do not have CUI, the government has defined a broader term: Federal Contract Information (FCI) in the Federal Acquisition Regulation. The protection requirements for FCI are fairly limited, and most modern IT systems can meet these requirements without much, if any, additional expense.

For CUI however, the bar is much higher. The NIST standard defines 110 distinct security requirements, each of which describes a "control" that the contractor must implement in order to safeguard CUI. Some of these requirements are fairly easy to satisfy, but others require a concerted effort and can drive overall cost.

In working with the NIST SP 800-171 standard since its publication in 2015, certain requirements have stood out as the most significant factors in the total cost of compliance.

Continuous Monitoring

The "Continuous Monitoring" requirement is often mis-understood and many MSSPs will claim that their 24x7 security operations center (SOC) meets this requirement. While a vigilant response to alerts is certainly helpful, this requirement has a broader scope than SOC monitoring. The requirement is to monitor all the security controls on an ongoing basis to ensure they remain effective. The standard states: "The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions." In practice this equates to a continuous monitoring plan with a mix of continuous (24x7 via automation) and periodic (daily, weekly, monthly, quarterly, and annual) checks. The standard also indicates that organzations must take "appropriate risk response actions." This means that if and when security safeguards fail or otherwise become less effective, the contractor must take a corrective action to restore effectiveness. Because of the broad scope and general implication that the entire cybersecurity effort must be monitored at all times and fixed whenever needed, this can be a major cost factor. There is almost always both an automation component (e.g,. Security Informaiton and Event Management [SIEM] tools for items monitored 24x7) and a human component (e.g., periodic assessment and inspection activities) that contribute to the cost of meeting this requirement.

Security Hardening

The next two items relate to system hardening: the practice of building and maintaining systems with the "Least Functionality" that is required and elimination of "Nonessential Functionality." Together, these two requirements represent a marked departure from the most prevalant build strategy used by IT operations teams: start with the vendor's default installation and add options/functionality as needed to make things work.

For most software, including operating systems such as Microsoft Windows, Apple MacOS, and Linux, the default installation script provided by the vendor configures the software with the most commonly used features enabled. This is convenient for both the administrator and the

The standard states: "The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions."

user because there's a high likelihood that the default build will work out of the box. However, this approach results in many software features being enabled by default, even if they will not actually be used. From a security perspective, having unused features enabled provides benefit for attackers who might try to exploit those features.

Cloud computing is much the same: default configurations are typically designed for out-of-the box convenience for new administrators. Cloud-based software often has dozens or, in the case of complex suites such as Microsoft365 or Google Workspace, hundreds of configuration settings that administrators can change.

In order to comply with the NIST standard, system builders need to take two time-consuming and detailed steps: they need to build the software in accordance with a "secure configuration baseline" and they need to disable all software components and features that are not going to be needed or used given the intended purpose of the system. These steps are known as "security hardening" of the system. Where running the default installation script may take only an hour or so, hardening of an operating system, database, application server, or cloud environment can take several days of administrator effort, including following detailed checklists with hundreds of configuration setting decisions and trial-and-error testing to be sure all required functionality works properly. In short, hardening tends to break things and it is challenging to determine which settings need to be changed to get things working. Any IT team or MSP that does not regularly build systems in accordance with security hardening guidelines will find the process extremely frustrating, and many lack the skills and tools needed to configure a system that is both functional and compliant.

Experienced compliance-aware IT teams and MSPs use standard build patterns (known as "gold images") that are replicated for many common system types. With this approach, the time consuming work of hardening is leveraged across many systems. These teams also use automated configuration verification tools, greatly reducing the time needed for trial-and-error testing.

Configuration Management

Items 4, 5 and 6 on the list are "System Baselining," "Security Configuration Enforcement," and "System Change Management." Where the hardening discussed above is typically done at the time of system build, configuration management is the ongoing process of tracking changes to the system over time. In order to be effective, configuration management is a discipline that must be followed by everyone and everything that changes hardware, firmware, software, and configuration settings. As with security hardening, this is a discipline that most small to mid-sized IT teams do not have. Most smaller teams function perfectly well with out of date network diagrams, incomplete software inventories, and, typically, no defined configuration baseline. Troubleshooting efforts tend to focus on trial and error methods to get things working again. Review and approval of changes is often informal, undocumented, or left as a one-person game-

time decision. Speed is prioritized over caution. Functionally, these methods are expedient and work just fine for keeping systems running and users happy. However, these quick-fix methods often leave gaping security holes in their wake and make it impossible to demonstrate compliance with federal cybersecurity mandates.

Adding a compliant configuration and change management function to an existing IT operation is often very expensive: new tools, new skills, culture change, and a loss of productivity. Careful well documented change management is time consuming, and time-to-results can suffer.

Large IT teams and some MSPs practice configuration management because it unlocks economies of scale as they seek efficiency in managing thousands of devices. Contractors that need to initiate configuration management have a classic "build versus buy" trade-off: Is it better to build this discipline where none exists or to buy services from an MSP where configuration management practices are built in?

Patching

While the first 80% of patching is relatively easy, the last 20% of the remediation effort can easily consume over 80% of the effort.

Item 7 is "Vulnerability Remediation." This requirement seems easy, but in practice can prove very challenging. The NIST standard requires companies to scan for vulnerabilities in their systems and applications. We didn't call this out as a cost driver because there are several cost-effective cloud-based solutions available that perform the scanning function quite well. It's the response to those scan reports that is deceptively difficult.

Once systems are built and stable – with all security hardening done – the number of vulnerabilities left would be small. This is true for a moment. But "new" vulnerabilities are discovered all the time. We say "new" in quotes because the vulnerabilities have often been in the software for some time, but are newly discovered, either by security researchers or by attackers. Virtually all software will have an ongoing stream of vulnerabilities that are discovered and announced, which contractors must fix.

Since most of these flaws are addressed by "patches" released by software vendors, it would also seem that meeting this requirement is a simple matter of maintaining a software support agreement with the vendor and applying patches as they are released. Some software today even has an auto-update feature where patches are automatically downloaded and applied. While it's true that a large portion of the vulnerability remediation effort can be addressed quite readily by built-in software update features, the 80/20 rules tend to apply. While the first 80% of patching is relatively easy, the last 20% of the remediation effort can easily consume over 80% of the effort.

High effort is needed for remediation steps that involve more than applying a software update. Some flaws will require manual configuration changes (e.g. Microsoft Windows Registry edits). Some flaws will interrelate with other software features such that applying the patch can break functionality. This can drive testing and troubleshooting costs. Some software changes will revert back when a system is rebooted, causing a vulnerability to re-appear.

The compliance requirement calls for remediation priorities and effort to be based on risk. The standard gives contractors latitude in the timing of patching, and low-risk vulnerabilities could be accepted indefinitely in some cases. But to meet the intent of the standard, contractors cannot simply ignore high-risk vulnerabilities that are troublesome or expensive to fix.

In looking at security budgets, it's important to have a realistic estimate of the labor cost associated with the "last 20%" of patching. This is another area where experienced IT teams have the edge. The flaw remediation efforts – the difficult part beyond routine software updates – has a steep learning curve. And, once a technique is proven, there is an economy of scale to apply that technique to a large number of similar systems. MSPs and cloud providers that utilize standard build images and have robust configuration management practices find it less costly to keep patching up to date. And experienced teams with a broader quiver of techniques at their disposal will spend less time on trial-and-error when dealing with the pesky flaws.

Another challenge is end-of-life software. Fixing newly discovered flaws is costly for software vendors and they typically only offer patches under support agreements for a period of time after software is released. Customers that want to use the software beyond that end-of-support or end-of-life date must either proceed without any new patches or upgrade to a newer version. From a compliance perspective, patching is required so the only viable option is an upgrade. This can translate into a "security compliance cost" if a contractor is forced to upgrade software that is still functionally adequate but is at the end of the vendor's support time window.

Encryption

Items 8, 9, and 10 relate to the use of cryptography to protect federal data by scrambling it so that it's unreadable. The standard mandates protection of "Data in Transit" as well as "Data at Rest." The standard also specifies that "CUI Encryption" must utilize laboratory-tested government-approved encryption methods. The latter is referred to by the shorthand "FIPS-validated encryption," referring to the federal Information Processing Standard (FIPS) used to evaluate cryptographic hardware and software. To meet these requirements, contractors must choose systems whose vendors have submitted their cryptographic modules for validation. The good news is that most major software vendors include validated cryptography in their products. What drives up the cost of compliance is that in essentially all cases FIPS validated cryptography is a non-default option. Administrators must elect to configure the software in "FIPS mode" and often this option must be selected at the time the software is installed.

The reasons FIPS mode is not the default have to do with performance as well as time-to-market. The government standards limit FIPS validated modules to specific encryption methods (algorithms and key lengths) that the government has approved. Non-approved methods often perform better, and customers not bound by federal requirements typically prefer the better performing encryption. Also, the FIPS validation process is expensive and time-consuming:

vendors must submit their cryptographic modules to approved independent laboratories for extensive testing and review. The validation step introduces a lengthy delay at the end of the vendor's development cycle. Non-approved modules can be brought to market faster and kept up to date easier. In practice, running software in FIPS mode to satisfy the federal requirements often means accepting sub-optimal performance and running slightly older versions of software. However, these compromises provide better security because the module has passed the rigorous testing.

As software is updated, contractors will sometimes need to choose between applying the update (to meet the Vulnerability Remediation requirement noted above) or sticking with the approved cryptographic module (to meet the CUI Encryption requirement). These choices require careful consideration, consultation with the vendor, testing, and perhaps seeking an exception from a government authority.

Running systems in FIPS mode is not the norm, and the details are often unfamiliar to IT administrators and vendor support personnel. While vendors generally do not charge extra for FIPS validated cryptography, the labor costs associated with building and maintaining systems in a non-default and unfamiliar configuration can add up. As with other items on the Top 10 list, experienced teams have the edge in terms of effort and cost. Once they have scaled the learning curve, this knowledge can be leveraged across large numbers of systems.

Experienced teams have the edge in terms of effort and cost. Once they have scaled the learning curve, this knowledge can be leveraged across large numbers of systems.

Multifactor Authentication

The requirement for "Multifactor Authentication" (MFA) did not make the Top 10 cost factor list primarily because it is included at no additional charge with most major cloud-based services and many companies have already started using MFA features. Although the technology is not costly to acquire or deploy, it deserves an honorable mention because MFA impacts the user experience which can cause soft culture-change costs to accrue. For the most part, user adoption of MFA has been slow over the past few years. As it has become more prevalent in consumer cloud services, users are starting to become familiar with the concept and will more readily adopt it in a corporate setting.

The NIST standard calls for MFA for every system that handles CUI. Local access by non-privileged users is the sole exception. In practical terms, this means that all logins other than local user workstation logins will need MFA: remote access; local area network access; and cloud service logins.

Contractors that rely on a mixture of cloud services from different vendors may find it challenging to deploy and support disparate MFA solutions. Single Sign-on solutions represent an additional cost, but may be worthwhile to simplify the user experience and keep support costs in check.

Attack Detection

At the very end of the NIST SP 800-171 standard is an oft-underrated requirement to "Identify Unauthorized Use." This requirement is essentially a catch-all that implies contractors need to notice when bad things are happening on their systems. Given that historically many intrusions go unnoticed by their victims until they are notified by law enforcement, satisfying this requirement can be harder than it looks.

This requirement bridges external and internal system monitoring, continuous monitoring (see above), and incident response. The typical security stack includes many different monitoring and detection systems. The NIST standard mentions: "intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, [and] network monitoring software." All these functions are mandated by earlier requirements in the standard. To meet this requirement, contractors need to generate alerts from these multiple sources and effectively assess and respond to each of them.

Whether this requirement represents a significant cost factor on its own depends to some extent on how the contractor has handled the preceding requirements. At a minimum, this requirement implies a level of effort to notice what's going on and react appropriately. This requirement is ultimately about security effectiveness. Did you simply "check the box" on the preceding requirements? Or are those safeguards effective in detecting and stopping attacks?

The tools and skills needed to discern normal from abnormal system activity are both esoteric and rare. Although automation, in particular behavioral analysis augmented by machine learning, is quite good at the detection task, it's necessary to perform human analysis to investigate which alerts represent unauthorized use (e.g., attacker activity) and which are false positives. Most small to mid-sized contractors cannot staff these specialized skillsets. MSSPs typically have the appropriate skillsets, but often lack contextual information about their customers' businesses that is needed to determine good from bad activity on the systems they monitor. Meeting this requirement often takes both MSSP services and engagement of the IT team (whether in-house or MSP) to resolve alerts: security and IT working together.

FedRAMP Cloud Services

The government's Federal Risk and Authorization Management Program (FedRAMP) is used to authorize cloud services for government use. Although the NIST SP 800-171 standard does not impose any specific requirements on cloud-based services, the government's mandate to follow FedRAMP security guidelines can be flowed down to contractors, even for their internal systems that handle CUI or other sensitive information. The DoD routinely places the DFARS 252.204-7012 clause in its contracts, mandating that all cloud computing handling CUI implement security requirements equivalent to the FedRAMP Moderate baseline.

There are about 300 FedRAMP authorized cloud services. This small quantity means there are thousands of cloud service providers that do not participate in the FedRAMP program. Although these non-authorized cloud providers may have fine security programs, if they cannot demonstrate that their security controls are equivalent to the FedRAMP Moderate baseline, contractors cannot use them to store or process CUI. The FedRAMP Moderate Baseline is more stringent than the NIST SP 800-171 standard imposed on contractors for non-cloud systems, with almost three times as many security requirements. Since many of these requirements are not standard commercial practice, such as the requirement for FIPS-validated encryption as described above, only cloud providers that have made an intentional effort to align with the FedRAMP requirements will have any chance of meeting all the requirements in the Moderate Baseline. In a practical sense, this means that contractors may need to switch cloud providers if any of their current providers are not FedRAMP authorized or able to document equivalence.

It's important to note that often Software-as-a-Service (SaaS) providers will host their cloud offering on one of the large Infrastructure-as-a-Service (IaaS) clouds such as Amazon Web Services or Microsoft Azure. The major IaaS providers are FedRAMP authorized, but this isn't sufficient. Even when a SaaS provider is leveraging a FedRAMP authorized hosting environment, it's necessary for the SaaS provider themselves to obtain FedRAMP authorization or demonstrate equivalence.

Whether the FedRAMP requirement is a cost factor for contractors depends on which cloud services they rely on for handling CUI. Many of the most popular cloud services, especially those that focus on the federal market segment, are FedRAMP authorized. Often SaaS tools used for IT support functions will be problematic. This area can encompass several different cloud vendors, and the tools often have access to systems with CUI. Contractors that use an MSP may find it difficult to obtain the transparency needed to even evaluate the toolset being used by the MSP and even more difficult to convince the MSP to change tools if one or more are not FedRAMP authorized or equivalent. A contractor in this position may have little option but to change to an MSP that is aligned with the federal cybersecurity requirements.

Beyond Compliance

In addition to the controls that are explicitly mandated, there are other security expectations placed on government contractors. In putting together the standards for nonfederal organizations, the government focuses closely on protecting the confidentiality of federal data (e.g., Controlled Unclassified Information) handled by the third-party companies in the federal supply chain. The government elected not to specify standards beyond this narrow focus. However, they did acknowledge a large number of security-related practices that are "expected to routinely be satisfied by nonfederal organizations without specification".

These practices are mandated within the government for its own systems, but for nonfederal organizations, these practices are left to the business judgement of the contractors. That doesn't mean they aren't important; rather the government is expecting that companies are sufficiently motivated by their own business needs and have these practices in place. These practices include such things as cybersecurity insurance, data backup and recovery capabilities, disaster recovery, and business resilience. Too important to ignore, they can be significant cost drivers to the overall cybersecurity effort.

As companies weigh cost and benefits, it's important to look at the entirety of the cybersecurity triad: confidentiality, integrity, and availability. Confidentiality, at least with respect to federal data is well covered by the federal mandates. Companies should do their own risk analysis that extends to protection of company intellectual property (that may not have a federal nexus) and the potential impacts of cyber threats on the ability of the business to maintain its operations.

The "Technical Debt" Factor

Contractors that rely on out-of-date IT systems will find that the cost of cybersecurity compliance is greatly inflated by the need to modernize their core IT systems as a prerequisite.

As noted earlier, it is not feasible to achieve compliance by bolting security onto legacy systems. Contractors that rely on out-of-date IT systems will find that the cost of cybersecurity compliance is greatly inflated by the need to modernize their core IT systems as a prerequisite.

It's very common for non-compliant practices to be highly entrenched, especially those that represent a convenience for users. Many companies are permissive when it comes to user devices such as laptops, tablets, and smart phones. They may allow use of employee-owned devices ("Bring Your Own Device" or BYOD), permit installation of personal-use software, and even grant administrator privileges on these devices to the users. These practices are inconsistent with compliance, and they can be difficult to dislodge.

In the recent past, BYOD and employee-managed devices were not feasible in a compliant system. Fortunately, modern device management software has improved such that it's now possible for companies to manage only the "work" aspects of a personal device, allowing the employee fairly free reign over their personal software and data. This capability is very useful since most employees already have a personal cell phone and do not want to carry a second device just for work functions.

As we've discussed, for core productivity, systems modernization is the right answer when it comes to both security and compliance. However, many contractors have specialized systems such as manufacturing control systems that are tied to machine tools and other parts of their factory infrastructure such that upgrades – and even patching – are often impossible. Contractors can and should take advantage of opportunities to segregate and isolate such systems. From a security perspective, it's valuable to limit access to these systems to minimize the risk of an attacker exploiting their (unfixable) vulnerabilities. Government treatment of such systems from

Cybersecurity is a good reason to pay off tech debt. Older, weaker systems are often targeted by attackers because their weaknesses are well known.

a compliance perspective is currently inconsistent, so the preferred approach is to "descope" such systems by segregating them from any CUI. If this is not possible (e.g., because the legacy systems themselves must handle CUI), then the next best strategy is to implement and document whatever segregation and isolation measures are feasible.

One area where it's reasonable to cut costs is by not migrating old historic data to newer systems. Often, it's cheaper to keep a legacy system running as an "archive" used only on the rare occasion when it's necessary to look up historic data. If this makes sense operationally, it's important to isolate the non-compliant archival system so that it is not targeted by attackers and does not cause problems on a cybersecurity audit.

In general, cybersecurity is a good reason to pay off tech debt. Older, weaker systems are often targeted by attackers because their weaknesses are well known and, if the software is out of support, cannot be fixed. Attackers will seek and exploit these systems if they can gain access. Contractors should upgrade or replace unsupported systems whenever feasible and isolate any systems that cannot be brought into compliance.

Common Mistakes

There are some well-meaning but inappropriate contractor actions that can drive up compliance costs. These are not the only pitfalls, but they represent common mistakes, that fortunately, can be avoided by well-informed decision makers.

Avoiding the risks of each of them, as outlined below, requires careful evaluation of each requirement as it relates to the contractor's situation. Consultants and MSPs can be of great value in this evaluation. In cases where a contractor finds themselves with questions that are not answered by the published guidance, it's appropriate to send in a request for clarification (or exception if appropriate) to the relevant government officials. For example, the DoD CIO has an e-mail address where requests of this nature can be submitted for review and adjudication.

Following are the common mistakes and how to avoid them.

Misinterpretation

The most common pitfall for those seeking compliance is mis-interpreting the government's requirements. Although we can all read NIST SP 800-171 and its accompanying assessment procedure, the government's wording intentionally stops short of specifying a solution. Contractors have latitude to determine how the requirements apply to their environment and how to best meet the requirements.

This is not an easy task and contractors often have questions about the intent or meaning of some requirements. The DoD's proposed CMMC program provides additional explanation beyond what is available in NIST SP 800-171. The government has also published both scoping and

assessment guidelines that can be of some help. Many of the requirements in NIST SP 800-171 contain cross-references to other NIST standards that provide detailed guidance. Comprehension and understanding of the nuances of the government standards is a full-time career path for a niche of cybersecurity specialists, and even those specialists can disagree on matters of interpretation.

Contractors that lack access to this esoteric and hyper-specialized knowledge face two significant cost risks. They might over-interpret the requirement and engage in "gold-plating" that is above and beyond the necessary expense to meet the government's intent. An example is issuing duplicative end-user devices (e.g., phones, laptops) such that workers need to use separate devices for their government-related work than they use for everyday corporate functions. While this sort of extreme segregation is secure and compliant, it is also overkill in most cases, imposing both monetary and user convenience costs that could be avoided.

Going the other way, the contractor might implement a solution that does not fully meet the requirements. In the worst-case scenario, the contractor might have to rip-and-replace their original solution with a compliant solution. An example is choosing a firewall or wireless router from a vendor that does not support FIPS-validated encryption. Although the device may be functionally similar and do a fine job of meeting all other applicable requirements, if the encryption provided is not FIPS-validated, the only practical path to resolve this gap is to purchase new equipment from a vendor that provides a FIPS-validated cryptographic module.

Delaying then Rushing

Our advice to those that are hesitant is to think in terms of technology life cycle. Invest now in the best available compliant solutions that will meet anticipated IT needs for the next three to five years.

Since government cybersecurity regulations are currently in flux, it is tempting to adopt a "wait and see" stance. With this stance, contractors hope to avoid early adopter mistakes. They want to let the market mature before committing themselves. However, this can backfire due to externalities: a key customer can threaten or cancel contracts; an attacker can exploit unsecured systems. In either case, the delay tactic can quickly turn into a costly rush job.

As noted earlier, the government's cybersecurity requirements – although evolving – are not new. Customers, whether the government directly or a higher-tier contractor, can be impatient once they discover that a member of their supply chain has been delaying compliance actions. They may impose strict deadlines to remediate gaps, and this can greatly limit the list of viable options, possibly forcing a contractor to select more costly solutions than they might select on a more relaxed timeline.

Although there are some possible benefits in letting others go first, in most cases the risks associated with delaying compliance outweigh them. Our advice to those that are hesitant is to think in terms of a three-to-five-year technology life cycle. Invest now in the best available compliant solutions that will meet anticipated IT needs for the next three to five years. And about halfway through that lifespan, evaluate the state of the market for the next generation of

compliant solutions. With this approach, contractors can demonstrate compliance in the near term and can still seek the benefits of an evolving maturing marketplace.

Cloud computing and managed services are both well suited to companies that need elasticity and incremental enhancements to adapt as they grow. Most contractors will benefit from minimizing the capital investment part of their IT budget by avoiding fixed on-premises equipment purchases in favor of subscription-based IT services.

Being Told What to Do

In the case where a contractor experiences a successful cyberattack, their insurance company will almost always get involved. The most common scenario is a ransomware attack, where the insurance company will often take charge of both the decision to pay the ransom and the recovery of company systems. Their goal is to act quickly to minimize financial impacts due to system downtime. Contractors may find their IT team pushed aside by a response team selected by the insurance company, with a narrow focus on re-building systems to avoid repeat ransomware incidents. It can be difficult or impossible to make strategic decisions about government compliance in the midst of an incident recovery. In short, this sort of incident can be both expensive and detract from compliance efforts.

As noted earlier, the government's cybersecurity regulations focus mostly on confidentiality of government data. Although some current ransomware gangs will steal and expose sensitive data to extort ransom payments, the primary responsibility to make systems resistant to ransomware attacks lies with contractors. Contractors are well advised to implement robust ransomware defenses in addition to the data confidentiality measures mandated by the government. It's also a good idea to coordinate with insurance company incident handlers ahead of an actual cyber incident to understand the resources they provide and how best to work together in case of an incident.

Incomplete Solutions

There are a lot of partial solutions on the market that address only specific requirements or even parts of requirements. A shared-responsibility model, where security and compliance actions are shared between the solution provider and their customers, is the norm in the marketplace. Where differences arise is in how the responsibilities are allocated. At one end of the spectrum are cybersecurity products. Products will have defined features, and it will be the responsibility of the customer to configure and use these features in a secure and compliant manner. At the other end are turnkey IT services, such as many MSP offerings, where a service provider retains responsibility for configuration and operation tasks, ensuring all the products in the IT stack are secure and compliant.

Both these solution types are viable, but the level of customer responsibility is dramatically different. In evaluating competing solutions, contractors need to ensure they understand the

entire operational picture including the costs and capabilities associated with actions they need to take themselves, recognizing that this could vary widely across competing solutions. All vendors of compliance-oriented solutions should offer a "customer responsibility matrix" or some variant that outlines exactly which requirements are addressed by their solution and which are the responsibility of the customer. If this information is not readily available from the solution vendor and aligned with the applicable government standards, it will be much more difficult for the contractor to conduct an apples-to-apples comparison with other solutions.

Overspending on Assessment

Contractors can and should allocate their available resources – time, people, money – at a high level into planning, building, and operating phases, ensuring that each gets adequate treatment.

In budgeting scarce resources, contractors must allocate adequate resources for the implementation and operations phases of their security and compliance journey. Because analysis and planning activities come first chronologically, it's common for contractors to spend money on planning tools such as Governance Risk and Compliance (GRC) software and consulting services such as a Compliance Gap Assessment without yet having a full picture of their total budget for IT, security, and compliance. In fact, it's arguably not even possible to gain an accurate understanding of all cybersecurity cost factors without first performing risk assessment activities.

While this is true at the detail level, contractors can and should allocate their available resources – time, people, money – at a high level into planning, building, and operating phases, ensuring that each gets adequate treatment. The cost of assessment activities can be managed by adjusting the scope and depth of the analysis. A good assessment will generally improve the "bang for the buck" of later spending. But contractors should be cautious in avoiding analysis for the sake of analysis.

Some cybersecurity consultants, used to working outside the confines of a federal compliance framework, may include elaborate risk analysis steps such as threat modeling and impact analysis which may be extraneous for contractors whose main goal is compliance with federal mandates. Similarly, many GRC tools help companies to select and focus their cybersecurity efforts based on either qualitative or quantitative analysis of risk. Again, this may be extraneous for a contractor's compliance effort.

The government has already done much of the up-front risk assessment work in selecting and tailoring appropriate control set for protection of CUI . While this doesn't entirely relieve contractors of the need to assess the cyber risks they face, it does shortcut the process. Since the government has specified controls that they deem appropriate, contractors can focus on selecting an implementation strategy for the prescribed items.

It's important at the start to be realistic about the total resources that are available to the company and keep up-front assessment and analysis costs in line, recognizing that money spent to identify gaps is no longer available to fix those gaps. And, in terms of security effectiveness as well as compliance, implementing protective measures is what matters most.

Smart Investing

Throughout this paper, we've mentioned numerous pitfalls and risks that can drive up cost, many of which can be traced to a complex marketplace for secure, compliant IT solutions. In short, IT vendors don't make it easy for contractors. While this is improving, the vast majority of software vendors and service providers in the marketplace today offer solutions that are all too easy to mis-configure or misuse in ways that violate good security practices and are not compliant with federal mandates.

Contractors all want to minimize their cost, but that doesn't mean they will accept shortcuts or inferior security. What they want is confidence. Confidence that if they spend a reasonable amount of money they will, in return, be well protected from both cybersecurity attacks and regulatory penalties.

Contractual Commitment of Compliance

In choosing their partners, contractors should insist on service providers – both cloud services and managed services – that will contractually commit to compliance with the very same standards and regulations the government is flowing down to the contractor. In cases where the service provider will have direct access to the government data, flow-down is likely mandatory. In cases where the contractor merely relies on the service provider as part of the overall security and compliance picture, it's still valuable if direct alignment with the applicable standards is committed to in the contract.

If a contractor receives a finding in an assessment, for example a DIBCAC or CMMC assessment, that relates to services they obtain from a third-party service, ideally the service provider will commit to correct the non-compliant service at no charge. Service providers that point to other non-federal security audits or certifications, for example AICPA SOC 2 audits or an ISO 27001 certification, may have very robust security programs and yet still be missing certain elements of the federal guidelines. Look for cloud providers to commit to at least the FedRAMP Moderate baseline and for MSPs and MSSPs to commit to NIST SP 800-171. For contractors that work for the DoD, DFARS 252.204-7012 has additional requirements beyond the NIST standard that service providers must align with and commit to meet.

Trusted Advisors

Contractors seeking certification under the CMMC program will need to hire a CMMC Third Party Assessment Organization (C3PAO) to perform the certification assessment. Today CMMC is a voluntary program mainly targeted at DoD contractors. Rulemaking is underway to add CMMC as a requirement for all DoD contractors, and a government-wide modification to the FAR is reported as being in the works. As these regulatory actions proceed, the majority of federal contractors will find themselves forming a relationship with a C3PAO.

However, independence rules prohibit C3PAOs from providing any advice to their assessment customers. While the C3PAO's assessors will be knowledgeable and well trained in the requirements, this restriction binds them to only assess whether the contractor's implementation meets or does not meet the CMMC standards.

Contractors should not look at the CMMC assessment as a "learning opportunity." Failing a certification assessment is a very expensive way to find gaps and deficiencies in a cybersecurity program, and of no value in determining how to best address those gaps. Rather, contractors should line up trusted advisor partners independent from their C3PAO well in advance of a certification assessment.

Failing a certification assessment is a very expensive way to find gaps and deficiencies in a cybersecurity program, and of no value in determining how to best address those gaps.

Unlike C3PAO assessors, these partners can be part of the solution, providing hands-on operational security support in addition to trustworthy advice. Contractors should look for partners that are closely aligned with the federal regulations and standards. Merely being knowledgeable in cybersecurity is not enough. There are many specifics of the government regulations that are not part of the general knowledge base for security practitioners working in the commercial sector.

Operational Costs

A recurring theme in this paper is that the ongoing cost of maintaining effective security and compliance is the dominant financial factor. As contractors consider their security spending, they should seek accurate estimates of the ongoing monthly costs, whether that is cloud service subscriptions, managed service fees, or employee labor costs. In the planning phase, consultants may say it's too early to know these costs. While that may be true at the very beginning, once candidate's solutions are being considered contractors will want to see estimates of one-time acquisition costs as well as ongoing operational costs.

Earlier we noted several requirements that are process-intensive: configuration and change management, continuous monitoring, patching, and detection. These are requirements that cannot effectively be met by set-and-forget methods. They are ongoing by nature. Any solution budget that does not explicitly include these functions should be questioned. It's very likely that the operational labor cost has not been fully considered in the budget. Asking hard questions about what is and is not included will help ensure that hidden costs do not surface after the fact.

Example Cost Model

The figure below depicts a budget for a common solution set adopted by small and medium sized contractors. This solution provides compliant cloud-based office-productivity IT services for typical knowledge workers, with full support for the IT and security operational functions provided by an MSP.

Small Med-Sized Contractor Cost Model

	Item	One-Time	Monthly
Company-Level Costs	Security and Compliance Program	$15,000-40,000	$2,500-7,500
	Cloud Environment	25,000-50,000	500-1,000
	Office Network	5,000-10,000	500-1,000
	CMMC Assessment (independent 3rd party)	30,000-50,000	0
Per-User Costs	Endpoint Mgt (security, patching)	$100-200	$50-100
	Mobile Device Mgt	0-50	0-20
	User Support	0-100	50-150
	Office Productivity Cloud (Full User)	200	50-100
	Office Productivity Cloud (GFE worker)	200	10-15

We present both company-level cost and per-user costs. Company-level cost factors relate to items that a company needs regardless of the number of employees it has. Per-user cost factors relate to items that each employee needs, where the cost directly depends on the number of employees in the company.

The cost model does not include the hardware cost of end-user devices such as laptops, phones, or tablets since most companies already own such devices (or at least have a good understanding of their cost). We did, however, include the per-user costs of building and supporting such devices in a secure and compliant configuration.

The example has broad ranges for some costs because all companies are different and because solution choice can affect overall cost. We feel these costs are representative of the vast majority of companies we have worked with, including a range of sizes and industry sectors.

This cost model focuses on the core office-productivity capabilities and does not include additional cloud-based Software-as-a-Service capabilities that companies may need: payroll, accounting, ERP, and specialized applications related to operations. If these cloud services will handle CUI, then contractors will need to budget for FedRAMP Moderate equivalent services and the services needed to configure and operate these additional cloud services in a compliant manner.

Companies that have specialized hardware such as manufacturing, process control, and other "operational technology" will have to budget for those in addition to the costs shown here.

Conclusion

Federal cybersecurity requirements pose a significant challenge to most members of the supply chain, and concerns about cost are widespread. The government is seeking to set the same bar for industry as it sets for itself, so it is incumbent on contractors to seek affordable solutions that provide the sort of robust security protection the government demands.

Contractors have many strategies to minimize the total cost of compliance without sacrificing security or the productivity of their workforce, including:

One-time costs get you compliant; Monthly costs keep you compliant.

- **Migration to a modern purpose-built IT architecture** sooner rather than later. Contractors should not try to bolt security onto legacy systems; rather they should migrate to compliant systems. This can be done all at once or in a phased approach depending on the level of change the business can absorb.
- For businesses that can **segregate people and/or data, enclaving** can be a good way to limit compliance scope. If government data, specifically CUI, is readily identifiable, or if workers associated with government contract efforts are a well-defined subset of the workforce, consider enclaving. In more homogeneous businesses, the effort to segregate may not be worthwhile.
- **Purchase cloud services** that can easily demonstrate compliance with the FedRAMP standards and that provide tools and/or configuration guides for using the service in a compliant manner.
- **Purchase managed services** from providers that will commit to ongoing compliance with the same standards that apply to their customers, preferably via a direct contractual flow-down.
- **Implement a standardized solution** with minimal customization. This unlocks the economies of scale that come from re-use of proven solutions. It's often worth adapting business practices to enable use of a pre-defined solution rather than embarking on a custom build.
- **Integrate IT, security, and compliance operational functions** into a "SecOps" approach. The federal standards emphasize operational maturity – the degree to which practices are institutionalized. This works best when security is "baked in" to the IT operation.

Repeated studies have shown that the level of implementation of security practices is not adequate. Contractors are experiencing significant pressure from their customers, whether that be the government or higher-tier contractors, to do better. Contractors that select trustworthy partners, choose solutions carefully, extinguish lingering tech debt, and adequately budget for ongoing operational costs will be most successful. Those are the contractors that will make smart investments that pay off in terms of both cyber resilience and competitiveness.

Footnotes

1. FAR 52.204-21
2. DFARS 252.204-7012
3. "Protecting Unclassified Information in Nonfederal Systems and Organizations", Rev 2, February 2020.
4. https://www.federalregister.gov/documents/2016/10/21/2016-25315/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for
5. CUI-Registry published by the National Archives.
6. FAR 52.204-21, Basic Safeguarding of Covered contractor Information Systems.
7. 3.12.3, "Monitor security controls on an ongoing basis to ensure the continued effectiveness of the Controls."
8. See NIST SP 800-137 for more detail.
9. 3.4.6, "Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities."
10. 3.4.7, "Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services."
11. Typically administrators will use industry recognized secure configuration guides such as CIS Benchmarks, vendor-provided checklists, or government issued Security Technical Implementation Guides (STIGs)as a starting point for hardening. NIST maintains a repository as part of the National Checklist Program.
12. 3.4.1, "Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles."
13. 3.4.2, "Establish and enforce security configuration settings for information technology products employed in organizational systems."
14. 3.4.3, "Track, review, approve or disapprove, and log changes to organizational systems."
15. 3.11.3, "Remediate vulnerabilities in accordance with risk assessments."
16. 3.11.2, "Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified."
17. 3.13.8, "Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards."
18. 3.13.16, "Protect the confidentiality of CUI at rest."
19. 3.13.11, "Employ FIPS-validated cryptography when used to protect the confidentiality of CUI."
20. FIPS 140-3, "Security Requirements for Cryptographic Modules." Modules evaluated under the older FIPS 140-2 standard are also still in use.
21. Validation is performed by laboratories working under the government's Cryptographic Module Validation Program (CMVP).
22. For example, DoD contractors are required by DFARS 252.204-7012 to seek adjudication of exceptions from the DoD CIO.
23. 3.5.3, "Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts."
24. 3.14.7, "Identify unauthorized use of organizational systems."
25. See FedRAMP Marketplace.
26. The DoD has published an FAQ that indicates how "equivalence" can be demonstrated by non-authorized cloud providers.

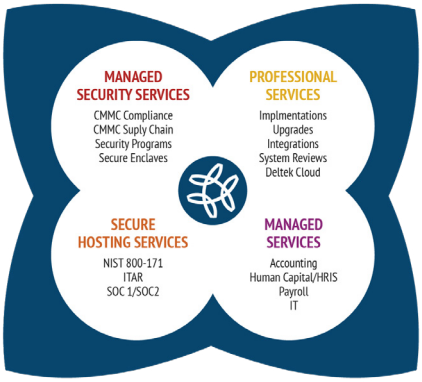
Footnotes Continued

27. NIST SP 800-171 Rev 2, Appendix E
28. By the federal Information Security Modernization Act of 2014 (FISMA) and NIST SP 800-53
29. osd.dibcsia@mail.mil. See the Defense Industrial Base Cybersecurity Portal for additional resources.
30. NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information."
31 See official CMMC website.
32. "CMMC Assessment Scope – Level 2", Version 2.0
33. "CMMC Assessment Guide – Level 2", Version 2.0
34. See NIST SP 800-171, Chapter 2 and Appendix E for an explanation of the tailoring criteria.
35. See AICPA & CIMA's SOC 2 web page.
36. See ISO's Information Security web page.
37. FedScoop, "Cyber AB launches voluntary CMMC assessment program for defense contractors," July 27, 2022
38. See OMB Fall 2022 Unified Agenda, Regulation Identifier Number (RIN) 0750-AK81 and 0790-AL49.
39. FedScoop, "New rule could impose CMMC-like cyber requirements for civilian agency contractors," April 5, 2023.

About NeoSystems

If your business is challenged by government regulations or your back office overly burdened, NeoSystems can help. As the experts in compliance and back-office functions, we can take accounting, finance, payroll, HR, IT and Information Security off your plate. We bring experience, best practices, technology, and compliance assurance to the table, allowing you to focus on your mission: winning new contracts and improving your bottom line.

We understand back-office, compliance, and cybersecurity so you don't have to.



- Proudly serving GovCons, Non-Profits, commercial and project-based firms
- Best-in-class technology partners with Deltek, Microsoft, Workday, SAP, Integrify, UKG

Grow ahead...We've got your back office.

NeoSystems®
11107 Sunset Hills Road, Suite 100 Reston, VA 20190
571 234-4940 | neosystemscorp.com | growahead@neosystemscorp.com