Case Study: Achieving DFARS Compliance

The Defense Federal Acquisition Regulation Supplement (DFARS) rule 252.204-7012 requires all non-Federal entities doing business with the Department of Defense that process, store, transfer or have access to controlled unclassified information (CUI) to comply with the security requirements published in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting CUI in Nonfederal Information Systems and Organizations*. Contractors and their subcontractors were directed to implement NIST SP 800-171 standards no later than December 31, 2017.

This case study examines Ascolta's journey in achieving NIST compliance for an existing DoD contract with one of the Military Services. Ascolta was a subcontractor to a larger system integrator, which instructed Ascolta to utilize a third-party service to report and monitor compliance. The software being developed for this contract was unclassified but contained controlled technical information (CTI). Because of this Ascolta was responsible for complying with DFARS rule 252.204-7012 as part of the contract flow downs from the contract prime.

Ascolta originally achieved NIST SP 800-171 compliance for this project by manually applying the 110 NIST SP 8500-171 security controls to our hardware based on-premise Contractor Integration Lab (CIL). This process took just over four months and cost approximately $60,000 in time and material to establish the baseline environment and did not include ongoing monitoring and management costs which are expected to cost an additional $40,000 per year. This was a relatively small lab environment with a small number of users, the costs could easily double for larger, more complex environments. As the contract progressed, the requirement to replicate the CIL in a secure and compliant cloud environment arose. Ascolta chose to utilize our own product called Greenfield, a NIST compliant cloud-based environment. The on-boarding process of the CIL into the Greenfield environment took four days and cost approximately $7,000 for initial compliance and is estimated to cost an additional $5,000 per month to sustain.

What follows is a comparison of the configuration of the physical and Greenfield based CILs through the compliance process.

Where to start?

The security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations has a well-defined structure that consists of basic and derived security requirements. The basic security requirements are obtained from Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, which provides high-level and fundamental security requirements for federal information and systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*. Starting with the FIPS Publication 200 security requirements and the security controls in the moderate baseline, the requirements and controls were tailored to eliminate requirements, controls, or parts of controls that are:

- Uniquely federal (i.e., primarily the responsibility of the federal government);
- Not directly related to protecting the confidentiality of CUI; or
- Expected to be routinely satisfied by nonfederal organizations without specification.

The combination of the basic and derived security requirements captures the intent of FIPS Publication 200 and NIST SP 800-53, with respect to the protection of the confidentiality of CUI in nonfederal systems and organizations.

Implementation of NIST SP 800-171 controls for both the physical and cloud-based CIL was accomplished by following the six-step process detailed in NIST SP 800-39, *Organization-Wide Risk Management*. The steps are: Categorize the System; Select the Controls; Implement the Controls; Assess the Controls; Authorize the System, and; Monitor the Controls. However, in implementing the controls for the cloud-based CIL, the Greenfield environment had done the heavy lifting for us for most of the steps, leaving us to focus on the assess and authorize steps.

Categorize the System

First, we had to determine what CUI was present, where it was located and who was using it. For the contract in question, an onsite physical lab environment, the CIL, was accessed virtually by developers where code was written, stored and tested. A government provided instance of Confluence hosted in the Defense Intelligence Information Enterprise (DI2E) was utilized to upload and store the finished code. The Confluence environment, being hosted in the DI2E environment, was not Ascolta's environment and therefore outside the required compliance boundary. It was determined that the servers in the lab and the network pathways for the lab to the DI2E servers needed to be NIST SP 800-171 compliant. It was then determined what users had access to the CUI in the environment to include the developers, system engineers and lab support personnel. Finally, the existing lab was assessed by reviewing existing documentation, data descriptions, and the existing system security plan (SSP), policies, procedures and process flows.

This step took the information systems security manager (ISSM) about three days in speaking with users, lab personnel and the program manager for the contract, and in reviewing the contract and existing architecture, policies and security documentation.

When implementing the cloud-based CIL in the Greenfield environment the same parameters existed with the exception of the physical architecture being replaced by virtual architecture in Amazon Web Services (AWS) U.S. GovCloud. The Greenfield environment is born in a documented compliant manner and comes with all required policies. Therefore, we were able to eliminate the steps of reviewing existing documentation, hardware and architecture configurations and the review of existing policies. This step in the Greenfield environment took us two hours.

Select the Controls

Normally the next step in the NIST SP 800-39 process would be to select the appropriate controls based on the categorization of the system. But for this situation the controls had already been selected by the DFARS rule requiring implementation of the controls contained in NIST SP 800-171. Although the controls are dictated there is a requirement in this step to

review them and determine which controls are not applicable and which controls may need to be added to provide additional protection. For the physical CIL this step took the ISSM an afternoon to review controls with the lab manager and IT manager. It was determined that there were several controls that were not applicable, all concerning wireless and mobile access, neither permitted in the lab architecture. For the Greenfield CIL, this step took a little over an hour, the Greenfield SSP listed non-applicable controls, but we still had to our specific requirements and insure there were no additional measures needed.

Implement the Controls

For the physical CIL this step is where the bulk of the time was spent and took the most effort. However, having an experienced ISSM and a couple of Certified Information System Security Professionals (CISSP) on staff helped immensely. Each of the controls had to be implemented, tested, verified and documented. Implementing some controls was as simple as documenting that established policies or procedures satisfied the control, others required changing the configuration, while some required architectural and design changes. It was fortunate that the lab was hosted in a facility that met all the physical security requirements, so no construction was required. A few controls required the purchase and installation of new hardware. Many of the controls required associated policies to be created, published and enforced. At the end of the exercise 22 new policies had either been edited or created. As controls were implemented their status was captured in a SSP, noting what actions were taken to implement the control and how it would be monitored to ensure compliance of the control going forward. For controls that were not initially implemented a Plan of Action and Milestones (POAM) was created providing a plan with a target completion date to implement the control.

All-in-all this step took three months, working with the ISSM, the Lab manager and the IT manager. At the end of the process we had a working SSP and a POAM with 43 open items.

For the Greenfield CIL this step took about a day. At birth the Greenfield environment meets 78 of the 110 controls and creating the environment took 15 minutes. The remainder of the time was spent entering users, verifying access requirements, completing and documenting training and ensuring the provided policies meshed with our existing policies. Having a pre-populated SSP saved us weeks of work during this step. Our POAM for the Greenfield CIL had five open items.

Assess the Controls

After all the controls were implemented in the physical CIL and the SSP and POAM created the effectiveness of each control was assessed to ensure it was in place, effective and measurable. Interviews were conducted for non-technical related controls, i.e. training, policy etc. and automated methods were utilized where possible for technical related controls and visually inspected for those remaining. This step took a week.

For the Greenfield CIL this step took an afternoon. Greenfield's compliance engine allowed us to quickly assess the majority of the technical controls, the remainder of the time was spent assessing the process and personnel controls.

Authorize the System

Upon completion of the assessment the results were briefed, and documentation presented (Policies, SSP and POAM) to senior management for approval. Preparations for the brief and the meeting totaled a week. Upon completion results were uploaded into the third-party tracking system that the prime required be used. This process, due to access issues, took two weeks.

For the Greenfield CIL this step was shortened, not only due to our experience with the third-party tracking tool, but due to the well organized and understandable documentation provided by Greenfield providing excellent briefing tools for senior leaders.

Monitor the Controls

Once initial compliance was achieved the next steps was to continuously chip away at the POAM to implement controls that needed more time or more substantial fixes. Additionally, in this step the system needs to be continuously monitored to ensure it remains compliant. New users must be trained, account access managed, and technical controls monitored to ensure they remain as intended. This step requires the ISSM to spend a few hours a week monitoring, maintaining and administering.

The Greenfield CIL provides a continuous monitoring feature that alerts users when technical controls are out of compliance and has mechanisms in place to assist in the monitoring of process and personnel-based controls. Additionally, the small number of open POAM items allowed us to focus on contract delivery rather than compliance enforcement.

Conclusion

Achieving initial compliance for the physical CIL took just over four months and cost $60,000 in time and material with an anticipated annual sustainment cost of $40,000. The cloud-based Greenfield CIL was provisioned and ready for use within a week for $7,000, a fraction of the initial compliance cost, and was fully compliant immediately. Annual costs for this type and size of Greenfield environment are $60,000, with less expensive environments available starting at $12,000 a year. The Ascolta Greenfield environment is created with security and compliance in mind; addressing NIST security controls in a single, easy-to-implement environment with:

- Continuous monitoring capabilities providing alerts when something occurs that takes you out of compliance
- Red Canary managed Security Operations Center (SOC) services that protect you and your data from security incidents and can assist in remediation efforts
- Completed security documentation to include policy templates, SSP and POAM.