AIRGAP

From NIST to CMMC Cybersecurity Compliance Guide for OT Cybersecurity

Compliance is no longer a matter limited to highly regulated industries. It's become an increasingly important part of cybersecurity programs for every business and organization.

That's because cyberattacks continue to evolve in scope and scale as bad actors target new industries. In the interest of protecting consumer data, lawmakers are quickly enacting legislation to provide extra protection to consumer's personal information. While this is a necessary move, it has also created new challenges, as organizations are often unsure of what compliance measures are needed.

That's why Airgap has assembled a Cybersecurity Compliance Guide for Operational Technology (OT) environments. This includes an overview of today's compliance requirements for a variety of industries and locations in uncarpeted and back-office areas, including Manufacturing, Transportation, Bio-Pharmaceutical, Healthcare, Banking, and Government.

Government business has seen an increase of its digitized data held in systems of subcontractors containing information related to finance, military, and other areas regulated by federal agencies.

To keep government data secure, Executive Order 13556 established the Controlled Unclassified Information (CUI) program to standardize the way federal contractors handle unclassified information which is known as NIST 800-171 standard. The US Department of Defense announced that its contractors must meet this standard or risk losing their contracts.

As your company wants to do business it is going to need to maintain compliance from more and more entities. Supply chain partners, and government entities are going to come to you and they are going to want to see your compliance plan. They will want to also see your progress across time.

Protect your organization from cyberthreats and learn how to stay compliant with NIST-CSF, NIST 800-53, NIST 800-171, NIST 800-207, and more. Learn all about key requirements and find additional resources to help make compliance easily understandable and actionable.

NIST-CSF - A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.
NST 800-53 - This applies to all federal data that is non-security data. So, all federal data.
NIST 800-207 - This standard discusses how to set up a zero-trust architecture.
NIST 800-171 - This is the standard for protecting CUI or controlled unclassified information.

These compliance frameworks are your guide to making this happen. This paper is your guide to make it even more simple. Because at the end of the day The National Institute of Standards and Technology (NIST) or Cybersecurity Maturity Model Certification (CMMC) is still just a framework. Yes, there are a series of controls. But you will be responsible for these controls. It will still be up to your organization to determine how to prioritize and implement these controls.

The purpose of CMMC was a continuation of the NIST standards. It was noted that cybersecurity standards are not set in stone. It is a moving target. And CMMC was designed to continue this process. And move with the changing requirements.

We have a series of controls we note below. And these are ordered by their NIST/CMMC components. And we determined which one of these can be mitigated or addressed by using the Airgap product. As you can see there are a lot of controls. And Airgap can address many of these. Either partially or completely.

NIST Controls to Notice

Let's talk about some controls from the NIST perspective and how these apply to OT Cybersecurity. This list is not exhaustive but will give you a starting place to look. It will show you some of the important controls to note and are specifically addressable by using Airgap.

NIST 800-171 Controls

Access controls 3.1.1,3.1.2, Limit information system access. 3.1.4, Separate the duties of individuals. 3.1.7, Prevent non-privileged users from executing privileged functions. 3.1.11, Terminate (automatically) a user session after a defined condition. 3.1.22, Control information posted.

Audit and accountability 3.3.4, Alert in the event of an audit process failure. 3.3.5, Use automated mechanisms to integrate and correlate audit. 3.3.6, Provide audit reduction. 3.3.8, Protect audit information and audit tools.

Configuration management 3.4.2, Establish and enforce security configuration settings. 3.4.7, Restrict, disable, and prevent the use of nonessential programs. 3.4.8, Apply deny-by-exception (blacklist) policy.

Identification and authentication 3.5.1, Develop identification and authentication policy and procedures.

Incident response 3.6.1, Establish an operational incident-handling capability.

Risk assessment 3.11.2, Scan for vulnerabilities in the information system and applications.

System communication and protection 3.13.2, Employ architectural designs, to promote security. 3.13.3, Separate user functionality. 3.13.12, Prohibit remote activation of collaborative computing devices. 3.13.13, Control and monitor the use of mobile code. 3.13.14, Control and monitor the use of Voice over Internet Protocol. 3.13.15, Protect the authenticity of communications sessions.

System information integrity 3.14.1, Identify, report, and correct information and information system flaws. 3.14.2, Provide protection from malicious code. 3.14.3, Monitor information system security alerts. 3.14.5, Perform periodic scans of the information system and real-time scans. 3.14.6, Monitor the information system including inbound and outbound communications. 3.14.7, Identify unauthorized use of the information system.

CMMC Level 3 Items

Audit and accountability 3.050, Limit management of audit logging functionality. 3.051, Correlate audit record review, analysis.

Configuration management 3.067. Define, document, approve, and enforce physical, and logical access restrictions.

Discussion and strategy

As you develop your NIST/CMMC policy, develop a System Security Plan (SSP). (A SSP serves as a comprehensive set of guidelines that your company will deploy to ensure proper cybersecurity hygiene. It will be based on the policies and procedures developed in your NIST/CMMC architecture. One critical element will entail how to address all of the issues, controls and compliance of this very detailed set of frameworks. Here are some tips in getting started:

Do not try to complete everything at once. It is impossible to complete all of NIST/CMMC elements within a certain narrow time range. At the very least it is not realistic. So, like many IT and OT projects, you will want to implement it for the least cost possible in the shortest time frame. What does this mean? It entails having a plan that is continual and dynamic. An SSP should include dates and responsibilities that are reviewed regularly and updated with new information or newly installed capabilities such as Airgap and Ransomware Kill Switch.

Work towards a goal into the future. Goals can often be moving targets, thus ensure that your SSP is adaptable and includes a Plan of Action with Milestones or a POAM. Don't expect to have this completed on day one.

Be able to show progress. This is critical from a practical standpoint as well as a legal and supply chain perspective. Finally, and most importantly, this is something that your compliance auditors are going to ask for again and again. When you get that call from a compliance auditor, you will want everything at your fingertips because in the event of a breach, you will be better prepared and have a greater likelihood to avoid an expensive lawsuit.

You want to address controls efficiently. With the list above you will realize the ability to address many of these controls with the Airgap Zero Trust Isolation platform. This is not only effective but productive and provides zero standing privilege security with full control and visibility. For instance, when someone in IT comes to you and says "how are we going to be able to monitor and divide, define and monitor physical access restrictions on our network, (CM 3.067), you will be able to depend on Airgap Zero Trust Segmentation to assist with this effort without having to build or buy an expensive set of defense tools.

"...cyberattacks continue to **evolve in scope and scale** as bad actors target new industries.

Reaching your goals

Your goal as an IT executive is to get the most security and productivity for the dollar as well as ensuring that your company is not the focus of the next security breach! This entails working smarter, not harder.
When external compliance auditors knock on your door, your goal is be prepared. The Airgap Zero Trust Isolation platform will go a long way to get you there.

The key to reaching compliance goals is to demonstrate a proactive plan, document progress, and report it all in a manner that follows the NIST/CMMC format and language.

Once all of these steps have been accomplished, you will need to demonstrate ongoing progress over time as well as have a clear plan of action that you and your corporate teammates can follow. Where will you be in one month? Next quarter? Next year? When is your next internal survey scheduled to ensure compliance and policing? Who is responsible at each step? What happens when one of your teammates leaves or is replaced? Can you continue to improve the plan without interruption or delay?

After the proper plan is in place, the next step will be to implement technologies, processes, procedures, and policies to take the most effective action in the least amount of time. This is where tools such as Airgap Zero Trust comes to play. As you can see by reviewing the NIST Standard, there are many controls that need to be addressed in a variety of areas, and the list of controls indicated above can be achieved by a successful implementation of the Airgap Zero Trust network segmentation technology. The need to compartmentalize and divide your network in a granular fashion is critical. This provides both network and application segmentation, the ability to detect abnormalities, and the capability to implement policies that facilitate protected areas within a VLAN. The latter is a powerful tool in accomplishing NIST compliance objectives, and Airgap can deliver!

Conclusion

When reviewing this paper, ensure that you use your NIST/CMMC guidelines. However, this paper can act as an effective guideline to implement the myriad of controls one faces with prioritizing, documenting, and maintaining an SSP. The end result should be a living plan that will accomplish your cybersecurity goals much more quickly and efficiently.

About Airgap

Airgap provides an agentless Anti-Ransomware platform to stop the spread of malware in the enterprise network. Our industry's first Ransomware Kill Switch™ locks down your most critical network assets at the first indication of compromise with complete control and policy enforcement over the device-to-device and device-to-application communication.

airgap.io

AIRGAP