Apptega

Preparing for CMMC Certification and Accelerating Growth

With Apptega, Cape Henry has moved from disparate spreadsheets to a programmatic approach to cyber- security and compliance

CAPE HENRY ASSOCIATES
PREPARING OUR ARMED FORCES

![Apptega logo]

Overview

- With spreadsheets leadership lacked visibility and confidence

- Apptega implemented as compliance system of record

- Immediately exposed unknown gaps in compliance with NIST 800-171

- Initial CMMC status quickly assessed

- Ready for CMMC audit ahead of schedule

- Easily demonstrating cybersecurity safety for DoD and contracting partners

- CEO has confidence in program efficacy and ability to meet commitments

LOCATION
Virginia Beach, VA

SPECIALITY
Manpower Analysis,
personnel analysis,
and training (MPT) services

————

"We now have the visibility needed to know the true status of our program at any time."

Ed Myers
Compliance Director
Cape Henry Associates

————

About Cape Henry Associates

Cape Henry Associates, based in Virginia, operates as both a prime contractor and subcontractor for the U.S. Department of Defense (DoD). The company is a [service-disabled veteran owned business (SDVOSB)](#) that specializes in manpower, personnel and training (MPT) services.

Founded in 2004, Cape Henry is a [SeaPort-e Prime Contract Holder](#), a contract vehicle that enables the company to provide a range of services including training devices, courseware development, front-end analysis (FEA) support, and more. The company specializes in innovative training and simulation scenarios.

Apptega

Cape Henry owns a Small Business Innovation Research (SBIR) technology stack called Lighthouse, a high-velocity learning environment (HVLE) that's designed to advance capabilities for training systems and requirement analysis. It powers the [Carrier-Advanced Reconfigurable Training System (C-ARTS)](#), which creates realistic training for Navy servicepeople in an augmented, virtual, and interactive environment. Almost 60% of Cape Henry's team are veterans, with almost 40% of them disabled veterans.

A Need for Robust Cybersecurity and Compliance Management

Because Cape Henry operates as both a prime and sub for the DoD, they have an obligation to protect Controlled Unclassified Information (CUI) shared within the Defense Industrial Base (DIB).

Prior to using the Apptega platform as its cybersecurity and compliance system of record, Cape Henry relied on spreadsheets, static documents, and share drives to manage its compliance program. As a result, Cape Henry's approach to cybersecurity, while effective, was disjointed. And compliance wasn't a dedicated focus for a single employee or team. Instead, the IT director and an assistant balanced compliance and security requirements in addition to a growing list of day-to-day tasks.

There were a number of challenges created by this approach, including difficulty reporting on compliance standards and an inability to quickly access data and other information to communicate progress andeffectiveness to the C-Suite.

CHALLENGES

Prior to using the Apptega platform as its cybersecurity and compliance system of record, Cape Henry relied on spreadsheets, static documents, and share drives to manage its compliance program.

In 2014, Cape Henry was affected by a phishing email attack that impacted several months of deliverables. The event highlighted several gaps in its cybersecurity program and although Cape Henry had a Plan of Action and Milestones (POA&M) report, company leadership lacked confidence in the report's completeness and the ability to execute the plan in a timely manner.

In 2016, Cape Henry earned certification of their ISO 9001:2015 quality management system, however internal audits of those static documents were challenging. As the business grew, the company quickly outgrew its cybersecurity infrastructure.

CHALLENGES

Dependence on spreadsheets was no longer effective and with increasing standards and mandates emerging for DoD contractors, Cape Henry leadership knew it was time for a change.

It became clear that Cape Henry needed to improve visibility into its cybersecurity posture. The dependence on spreadsheets was no longer effective and with increasing standards and mandates emerging for DoD contractors, Cape Henry leadership knew it was time for a change. They needed an improved cybersecurity approach and asked Ed Myers to step up as the company's Compliance Director.

CMMC and Increasing Requirements for Protecting CUI

As the company made gains on achieving NIST 800-171 standards, the government announced the rollout of the new [Cybersecurity Maturity Model Certification (CMMC)](#), which will be required for all new contract bids and renewals.

In the first quarter of 2020, Cape Henry began its search for a cyber-security management and compliance platform that would:

✓ Serve as a single source of truth for its program

✓ Help to quickly and thoroughly identify program gaps

✓ Help manage remediation tasks and projects and promote accountability

✓ Provide the visibility needed by the compliance director and other executives

✓ Enable streamlined audits

✓ Successfully facilitate the CMMC certification process

Cape Henry also wanted to find a system that was easy to use and provided by a vendor with a vested commitment to its success. After a broad search, the company decided that Apptega — both the company and the platform — provided the best fit for its needs.

Did you know?

CMMC is an extension of the CUI program created by the U.S. government in 2010 to standardize how contractors and service providers handle non-classified, but protected government information.

The Apptega Solution

Among many other capabilities, Apptega supports more than a dozen cybersecurity and privacy frameworks including NIST 800-171 and CMMC, both critical to Cape Henry as a DoD contractor.

Cape Henry kicked off its Apptega implementation with a goal to achieve full compliance with NIST 800-171 and CMMC by early September 2020. Team members wanted to be ready for a CMMC audit as early as October.

Upon uploading its NIST 800-171 data into Apptega, team members were pleased to discover they were already at 92% of full compliance with the NIST standard. The Apptega platform also immediately exposed some additional gaps that were previously unknown.

APPTEGA BENEFITS

"The biggest advantage with Apptega is in the dashboards and reporting. We now have the visibility needed to know the true status of our program at any time."

According to Ed Myers, Cape Henry Compliance Director, "With Apptega, we're able to take a cost-effective DIY approach to cybersecurity readiness and compliance. The built-in guidance for each of the sub-controls helps us quickly compare what we are actually doing with what we need to be doing. Gaps are readily identified, and remediation tasks are set up in the platform to give us a 360-degree view of our status and plans."

Monitoring the status of projects and receiving automated notifications for overdue tasks, Myers uses the Apptega platform to hold team members accountable to commitments.

"The platform is great for managing day-to-day tasks and with it, our ability to accurately predict the completion of our projects is significantly improved," Myers said. "But the biggest advantage with Apptega is in the dashboards and reporting. We now have the visibility needed to know the true status of our program at any time. Our CEO is very happy now and has confidence in our ability to meet our commitments as well as the overall completeness and efficacy of our cybersecurity program."

CMMC Implementation

Implementation of the CMMC framework began with the unique Harmony feature in Apptega. This allowed Cape Henry to crosswalk the NIST 800-171 framework with CMMC, requiring only a few clicks.

The result was a new combined framework with all the overhead of redundancies between NIST 800-171 and CMMC consolidated.

With the frameworks harmonized, the cybersecurity team was pleased to see that they were already at 57% of full compliance with CMMC based on their NIST 800-171 status. With a high degree of confidence, they could also see all the CMMC gaps that would need to be remediated.

Myers used the Apptega platform to monitor the status of CMMC remediation projects and overdue tasks, enabling him to hold team members accountable to their commitments. The target for completing all CMMC remediation tasks is January 5th and they are comfortably on track for completion ahead of schedule in Mid-December.

APPTEGA BENEFITS

With the frameworks harmonized, the cybersecurity team was pleased to see that they were already at 57% of full compliance with CMMC based on their NIST 800-171 status.

Competitive Advantages

With the Apptega platform, Cape Henry can instantly produce detailed evidence of its readiness for CMMC Level 3 certification.

Although the formal certification process with a CMMC Certified Third- Party Assessor Organization (C3PAO) is unlikely to get started before early 2021, Cape Henry is already using their preparedness to grow and sustain the business.

APPTEGA BENEFITS

Cape Henry is using the objective evidence within Apptega to demonstrate they are the safe choice and win more business.

In situations where Cape Henry serves as a flow-down subcontractor in large DoD contracts, the upstream contractors prefer to work with subcontractors deemed safest in terms of protecting sensitive CUI and also minimizing the risk of losing a contract. A contract that will eventually require certification to CMMC Level 3 may be at risk if the subcontractor(s), in addition to the prime contractor, cannot achieve the proper certification. Cape Henry is using the objective evidence within Apptega to demonstrate they are the safe choice and win more business.

Cape Henry also participates in a unique DoD contract with two other companies, all operating at the same level—none designated as a prime or sub. Within this triad, any of the companies may take the lead or collaborate with the other companies on specific projects. Again, safety becomes critical for sensitive CUI and this is an advantage for Cape Henry.

Cape Henry also relies on small subcontractors with five or fewer employees in each organization. In most cases, achieving CMMC Level 3 certification is cost-prohibitive for these small organizations. To ensure they continue to benefit from the unique and important services of these specialty subcontractors, Cape Henry has been able to bring them in, under the protections of its cybersecurity program. This symbiotic relationship, enabled by its robust cybersecurity program and the Apptega platform, helps ensure that Cape Henry can continue to deliver on contractual commitments with minimal risk.

"Because of our proactive CMMC preparation using the Apptega platform, we can easily demonstrate Cape Henry's cybersecurity safety for the DoD and any of our contracting partners in the DIB," Myers explained. "This has already become a meaningful competitive advantage for us as CMMC scrutiny has increased up and down the supply chain."

Apptega for Cybersecurity and Compliance Management

Apptega plays a vital role in helping Cape Henry Associates mature its cybersecurity posture and provide comprehensive insight into its program.

With the help of the platform, Cape Henry is confident in its ability to successfully complete its CMMC certification and is poised to adopt additional cybersecurity frameworks as needed.

Like Cape Henry, Apptega is helping other DoD contractors and CMMC Registered Provider Organizations (RPOs) as they develop specialized cybersecurity programs based on best practices including CMMC, NIST, ISO, GDPR, HIPAA, CIS, and more. The platform can help make your cybersecurity and compliance management processes more efficient and help you improve the maturity of your program without added resources. Contact an Apptega advisor or visit apptega.com today to learn more.

Available Frameworks

Industry & Vertical

SOC 2
PCI DSS
23 NYCRR 500
SEC

Government

CMMC
NIST 800-171
NIST 800-53

Standards-Based

ISO 27001
NIST CSF
CIS V7

Privacy

CCPA
GDPR
HIPAA

Custom

Custom Frameworks

About Apptega

[A perennial G2 leader across various cybersecurity categories](), Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.

2. Build and manage world-class cybersecurity and compliance programs for their clients.

3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.

4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit [apptega.com]()

Visit apptega.com