BDO USA

ARTICLE

April 14, 2023

The BDO GovCon Week Ahead - April 2023

April 17, 2023

In an Era of Endless Cyber Threats, What Does the Next Iteration of Security Look Like?

With 2023 well underway, the Cybersecurity and Infrastructure Security Agency (CISA) has begun to focus on its 2024 budget request, with a major restructuring on the horizon. For the past 15-20 years, CISA has been utilizing, and continuously developing, the National Cybersecurity Protection System (NCPS), more commonly known as EINSTEIN, to defend federal agency networks since the Department of Homeland Security's (DHS) inception in 2003. While parts of EINSTEIN will remain, CISA plans to transition its predominantly detection-based system, into a more analytical approach known as the "Cyber Analytics and Data System," or CADS for short.

Per the DHS' 2024 proposed budget, CISA plans to transition NCPS' "intrusion detection and

intrusion prevention capabilities," into its new CADS program. The program will "provide tools and capabilities to facilitate the ingestion and integration of data as well as orchestrate and automate the analysis of data that supports the rapid identification, detection, mitigation, and prevention of malicious cyber activity," all of which contributes to the defense of the Federal Government's information technology infrastructure from cyber threats.

In an interview with Federal News Network, CISA's executive assistant director for cyber security, Eric Goldstein, elaborated on additional features the new CADS system will wield in the pursuit of data security. To start, the system will integrate data from "public and commercial data feeds; CISA's own sensors such as Endpoint detection and Response, Protective [Domain Name System], and our Vulnerability Scanning service, which has thousands of enrolled organizations across the country; and data shared by both public and private partners," said Goldstein. CADS will also allow for greater efficiency and better analysis of data as it's single repository for data removes the needs for analysts to manually compare data and threat information stored in different systems, as is done in the current environment.

As data security advances, so too do the threats to the Federal Government's information technology infrastructure. Now more than ever, it is essential for data security to forge ahead in the race of advancement in order to edge out malicious threats. CADS, described as a "system of systems" will provide CISA with a central data security hub that allows for additional software development, succinct data analysis, and an agile environment that supports the rapidly expanding agency.

Contractors which specialize in cybersecurity should be on the lookout for proposals from CISA for assistance with the new CADS system after September 2023.

For more information, visit:

- cisa.gov/einstein
- Department of Homeland Security Cybersecurity and Infrastructure Security Agency Budget Overview

April 10, 2023

Bridging the Valley of Death: Office of Strategic Capital

and Small Business Administration partnership

Back in December 2022, the Department of Defense (DoD) established the Office of Strategic Capital (OSC) in response to a long-standing problem flagged by defense companies in the private sector – the "valley of death." This term is commonly referred to in the industry as the often-long-term gap between development and actual production for new technologies. Historically, the technology companies have had a difficult time securing long term "patient" capital which results in an inability to bring critical technology to scale for military use. Furthermore, many of the technologies that are vital in developing future military capabilities are not directly procured by the DoD. Thus, this clearly indicates the lack of capital support from existing procurement programs to meet the needs of those companies.

Due to DoD's legal limitations, the OSC plays a key role in bridging the gap by linking companies that have essential defense capabilities with sources of private capital. By working with private sector partners outside the Pentagon, the OSC is able to help further DoD's investment priorities. It is particularly important when it comes to hardware such as semiconductors since there has been a trend away from investing in deep or critical technologies in favor of software which has lower risk and higher returns. In efforts to encourage investment in advanced materials and cutting-edge technology, the OSC plans to first partner with the Small Business Administration's Small Business Investment Company (SBIC) program.

Unlike the DoD, SBA can leverage the full faith and credit of the U.S government to increase the pool of investment capital available to innovative companies. Through the SBIC program, the SBA provides loans and loan guarantees to private investors aiming to boost their confidence in making investments in more critical technologies vital to national security. Compared to several other countries such as China where there may be heavy government intervention in the private sector, the U.S. takes on a partnership approach through empowering investors to make their own choice. Looking to its continued development, the OSC plans to partner with other agencies in the future to support the extension of loans in scaling innovative and advanced technologies.

April 3, 2023

Don't Ever Throw Away Your Paperwork

Per the Contract Disputes Act (CDA) the statute of limitations for a claim by the Federal

government against a contractor, or a contractor against the Federal government relating to a contract, is six years (41 U.S.C. §§ 7103(a)(4)(A)). The law concerning the six-year statue continually evolves however and has become less rigid resulting in long term issues for defending against claims. All of this came to a head recently in the Armed Services Board of Contract Appeals decision in February 2023 concerning a request for summary judgment by Beechcraft Defense Company, LLC against a claim made against it by the Defense Contract Management Agency (DCMA). A little background will help.

The most significant change concerning the CDA statute of limitations occurred in 2014 when the U.S. Court of Appeals for the Federal Circuit held in Sikorsky Aircraft Corp. v. United States that the statute of limitations is no longer jurisdictional but is an affirmative defense. Prior to Sikorsky the claimant bore the burden to prove that the statute of limitations did not apply (did not have jurisdiction). An affirmative defense means that the party seeking to invoke the statute of limitations bears the burden of proving that it does apply (that the claim accrued or started more than six years before its assertion by the claimant). One of the outcomes of the Sikorsky ruling is that the boards of contract appeals and Court of Federal Claims are not barred from hearing cases involving untimely claims.

A quick review of the timeframes of the documents involved in the Beechcraft case (ASBCA Nos. 61743, 61744, 61745 dated 2.02.2023) illustrates the issue with untimely claims. The Beechcraft case revolves around the following:

- Three Defense Contract Audit Agency (DCAA) audit reports concerning Cost Accounting Standards (CAS) non-compliances issued in June 2011.
- A fourth DCAA audit report issued in June 2011 concerning Beechcraft's forward pricing rate proposal for 2011-2015. The audit report considered the alleged CAS non-compliances to have a limited impact on the proposal and DCAA believed the proposal to be an acceptable basis for negotiation of fair and reasonable forward pricing rates.
- At some later point (the record is unclear exactly when) DCMA requested that Beechcraft submit general dollar magnitude (GDM) proposals related to the CAS non-compliances. Beechcraft did so in April 2015. At DCMA's request Beechcraft resubmitted the GDM proposals in July and August 2016. DCAA audited the proposals throughout 2017.
- In May 2018 DCMA issued a contracting officer's (CO) final decision regarding the non-compliances which Beechcraft timely appealed in August 2018.

Beechcraft asserts that the statute of limitations began to run in June 2011 when DCAA issued its reports on the non-compliances and the forward pricing rate proposal and that the CO's final decision in 2018 was beyond the six-year period. DCMA asserts that the statute began to run when Beechcraft submitted its GDM proposals in 2015.

Beechcraft sought a summary judgment which the Board denied due to a lack of evidence. The Board's decision does not prevent Beechcraft from presenting additional evidence in the future which Beechcraft will likely do. As a result, the case is ongoing twelve years after the original DCAA audit reports and could continue on for another two or three years.

For more insights concerning this case read the interview with Zach Prince, Haynes Boone law firm partner, by Tom Temin in his article titled "Defense claims against contractors have a shelf life of infinity" (link below).

Defense claims against contractors have a shelf life of infinity | Federal News Network