wiley

NEWSLETTER

Challenges and Opportunities for the U.S. Department of Homeland Security's Expanding Role in Government-Wide Procurement Policy

February 2021

The U.S. Department of Homeland Security (DHS) has been central in federal cybersecurity policy for years, as an important non-regulatory body that convenes the private sector, works across agencies, and protects information sharing with and between the private sector. We expect DHS to increase its influence on federal procurement in the coming years, both as a network security advisor to most federal agencies and as a purchaser of networking, security, and cybersecurity services. Contractors should keep an eye on DHS's expanding role in procurement policy, particularly as new leadership takes the reins of the agency.

Recent legislation and Executive Orders have increased DHS authority, largely in the Cybersecurity and Infrastructure Security Agency (CISA). These actions make DHS a key participant and advisor to bodies like the Federal Acquisition Regulatory (FAR) Council, Federal Acquisition Supply Council (FASC), the Information and Communications Technology (ICT) Supply Chain Task Force, and many other activities that will impact the private sector.

DHS/CISA Have Broad Authorities for Federal IT and Network Security

DHS and CISA have broad authority to secure the networks and IT equipment utilized by civilian federal agencies. As a result, CISA has a central and coordinating role in federal IT procurement.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Practice Areas

Government Contracts

Telecom, Media & Technology

- Under the *Federal Information Systems Modernization Act* (FISMA), 44 U.S.C. 3551-3558, CISA has a central role securing the information and information systems of federal civilian agencies. CISA is responsible for developing and coordinating government-wide policy and guidance, and offering technical assistance and capabilities to increase the security of federal agency networks. CISA also can issue binding operational directives and emergency directives requiring agencies to implement security measures on information systems to protect against vulnerabilities, risks, and security threats.
- CISA also helps coordinate the Government's assessment of supply chain risk in procurement. Under the relatively new *Federal Acquisition Supply Chain Security Act*, 41 U.S.C. 1321-1328, CISA has a central role on the Federal Acquisition Security Council (FASC), which was established to oversee security-related decisions in federal IT procurement and to address supply chain related risks to federal information systems. In addition, the *Cybersecurity Information Sharing Act of 2015*, 6 U.S.C. 1501-1533, requires DHS to establish a process for sharing cyber threat indicators with both the federal government and private sector entities.
- Information sharing and technical assistance are additional functions. The *Cybersecurity and Infrastructure Security Agency Act of 2018,* 6 U.S.C. 651-674, establishes CISA as the principal agency responsible for sharing cyber threat information, and authorizes CISA to provide both cybersecurity technical assistance and incident-response capabilities to agencies upon request.

Recent Executive Orders, Legislation, and Policies Give DHS a Larger Role in Procurement

Recent executive orders and policies have given DHS and CISA responsibilities that will affect procurement across government. A few examples are discussed below.

DHS Will Drive Government Requirements for Position Navigation and Timing (PNT). Executive Order 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services*, was issued on February 12, 2020. It requires the government to develop "PNT profiles" for critical infrastructure sectors by February 18, 2021. Sector-specific agencies then have 90 days to "develop contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services."

DHS has a leading role, along with NIST, in building out PNT responsible-use profiles. It is unclear how the agency expects its work to be used in procurement, despite the EO's call for procurement changes. Presumably, the FAR Council will promulgate FAR clauses to add new requirements into contracts for products and services that integrate or use PNT services. Even though companies will eventually be charged with meeting new contract obligations, there have been few public discussions about how DHS's work on PNT will influence procurement. Without public engagement from DHS, affected companies may not have an opportunity to provide input until the FAR Council issues a proposed or interim rule. Industry should look for opportunities to have DHS explain to the public and the contracting community, in each sector it is examining, how its profiles will inform procurement policy.

DHS will Drive Procurement Changes in Bulk Power Systems. Executive Order 13920, *Securing the United States Bulk-Power System*, which was issued on May 1, 2020, declared a national emergency under the International Emergency Economic Powers Act (IEEPA) with respect to the threat to the United States bulk-power system and sought to protect the security and integrity of the bulk-power system electric equipment. The EO established an interagency Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security, which includes the DHS. The first responsibility for the Task Force is to develop consistent energy infrastructure procurement policies and submit recommendations to the FAR Council.

The Task Force has not provided significant public communication about how future procurement obligations will reflect the Task Force's recommendations. On January 20, 2021, the new Administration issued an Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis, which temporarily suspends implementation of the Bulk Power EO and directs OMB and the Department of Energy to evaluate replacing the order.

DHS Controls Procurement of Security-Related Goods and Services Across Government. DHS and CISA play a role in the OMB-led *Category Management* initiative aimed at eliminating redundancies in federal procurement. DHS is the lead agency for the Security and Protection category, which includes Security Services and in April 2020, OMB designated CISA as the government-wide Cybersecurity Quality Service Management Office (Cyber QSMO). In this role, CISA manages a marketplace of centralized cybersecurity services that agencies may use. One of the first services offered is a Vulnerability Disclosure Platform that will help manage vulnerability disclosure practices across government and will be available to agencies in Spring 2021. Additionally, CISA will offer Security Operations services that will be provided with the Department of Justice. CISA has substantial discretion in prioritizing approaches and selecting partners and may need additional resources to oversee growing government requirements. To ensure that CISA can take advantage of new technologies, mitigate post-award industry consolidation and maximize competition for agency procurements, Cyber QSMO platforms and contract vehicles should incorporate on-ramps at regular intervals.

Binding Operational Directives Will be Influential. CISA has unique authority in binding operational directives (BODs) and emergency directives (EDs) to direct certain agencies to deploy information security protections or mitigations in response to a threat, incident, or vulnerability. 44 U.S.C. 3553. CISA has used this authority several times over the past several years, with BODs requiring removal of Kaspersky products from federal systems, mandating vulnerability disclosure policies for internet-facing federal systems, and the emergency directive implementing mandatory patches and mitigations in response to the attack on the SolarWinds network management tool. This authority feeds into acquisition by giving CISA a consultative role to OMB in security requirements for federal systems. CISA could exercise this authority more frequently to impact federal IT security posture, including critical incident and threat response.

New DHS Leadership Will Face Numerous Challenges in Procurement

As DHS leaders grapple with the extent of the agency's role in procurement policy, several areas merit focus:

- *DHS leadership should consider how it wants to influence procurement policy.* Significant changes to federal procurement and efforts to shift private markets using federal purchasing power should be undertaken with care. DHS should preserve longstanding policies promoting competition in contracting, technical neutrality, use of private standards, and the reliance where possible on commercial solutions and offerings, rather than bespoke government solutions.
- *Communication with affected industry is critical*. Private sector entities may carry the primary responsibility for cybersecurity and other protections of critical infrastructure. These obligations are imposed through clauses incorporated in a company's contracts with the Government.
- *Transparency about DHS's procurement priorities and work with the FAR Council will lead to better outcomes*. In some instances, there has been little transparency into cyber or supply chain obligations that may be imposed on private companies, leaving them unable to prepare. A lack of transparency can result in FAR clauses that do not reflect how companies do business or differences between sectors, and there is little opportunity to comment. This is evident in the implementation of Section 889 of the FY2019 NDAA, limiting procurement from certain Chinese companies, which has been controversial and criticized as overbroad, unclear, and burdensome.
- *DHS can play a key role in deconfliction and coordination*. Numerous agencies have been addressing supply chain security, and those policies overlap and are sometimes inconsistent. For example, Section 889 and its implementing regulations prohibit contractors from using telecommunications equipment or services that use equipment or services from Huawei, ZTE, or other Chinese companies. At the same time, the State Department launched the Clean Network initiative, including Clean Path to ensure communications networks to and from U.S. diplomatic facilities do not use equipment from "untrusted IT vendors." Through participation in groups such as FASC and the ICT Task Force, DHS can promote a consistent, government-wide approach to supply chain security.