THE
COALITION
FOR GOVERNMENT PROCUREMENT

STATEMENT OF ROGER D. WALDRON

PRESIDENT OF THE COALITION FOR GOVERNMENT PROCUREMENT

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION OF

THE COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

UNITED STATES HOUSE OF REPRESENTATIVES

NOVEMBER 29, 2023

Good afternoon, Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee. Thank you for the opportunity to appear before you to address the federal software supply chain.

The Coalition for Government Procurement is a non-profit and non-partisan association of firms selling commercial services and products to the Federal Government. Our members collectively account for more than $145 billion dollars of the sales generated annually through government contracts, and span small, medium, and large business concerns from across the commercial market. They include commercial software firms, cloud providers, systems integrators, and IT hardware suppliers. As such, they are well-aware of the challenges involved in addressing vulnerabilities in the federal software supply chain.

The threat from near-peer adversaries and other bad actors has made cybersecurity and supply chain risk management fundamental to federal procurement and the commercial sector. Recognizing the importance of this matter, there are three points I would like to make.

First, the government should continue prioritizing buying commercial solutions where appropriate. The Federal Acquisition Streamlining Act of 1994 established a preference for the acquisition of commercial items. This preference reduces risk, increases competition, improves pricing, provides greater access to innovation, and it improves security. Commercial software firms recognize that security failure risks reputational harm which would translate into the loss of business. For this reason, drawing on their experience across industry sectors, like healthcare, banking, finance, and energy, they understand that they must invest in security, and they do so. Government should capitalize on this experience.

Buying commercial allows the federal government to leverage commercial expertise and investments in security and functionality. It also ensures that the government stays current with security solutions in a dynamic cyber-threat environment. As the federal cybersecurity framework continues to evolve and mature, maintaining long-held preferences for commercial items will mitigate risk, increase competition, and deliver functionality for the federal customer.

Second, cybersecurity requirements, reporting, and other administrative compliance regimes should not burden commercial firms unnecessarily. Some requirements are necessary, but unnecessarily burdensome requirements drive companies out of the government marketplace, reducing government access to commercial markets. As the Administration's recent draft memo on The Federal Risk and Authorization Management Program (FedRAMP), stated:

> "unthinking adherence to standard agency practices in a commercial environment could lead to unexpected or undesirable security outcomes."

Some government mandates for certifying commercial products could create compliance risk when the mandates are not required outside of government. The "false certification" exposure associated with such government-unique requirements raises costs and undermines the incentive to work with government, while doing little to improve security. The government should accept commercial standards wherever possible and required certification should focus on whether what is being provided actually meets those standards.

Third, and finally, the federal cybersecurity and software supply chain framework is in a state of flux, and coordination is needed. There are various pending rules and regulations, like FedRAMP, CMMC, NIST 800-171, SBOMs,

proposed FAR cybersecurity clauses, Section 889, and the Federal Acquisition Security Council (FASC), all of which are in various stages of government review and/or public comment.

Communication and dialogue between government and industry is vital to ensuring that all these moving parts work together, providing a rational, effective, and not unnecessarily burdensome security framework. For example, a software bill of materials or SBOM can play a meaningful role in identifying vulnerabilities in the software supply chain, but current and proposed government requirements leave too many unanswered questions and ambiguities, making it possible for different interpretations by different agencies. Current proposals would require an SBOM and attestation for major updates to existing software. What is a major update? What about frequent, but small, updates? What is the role of open source and third-party software? Even the commercial market has not established best practices for SBOMS. We suggest that the government continue to seek feedback on these and other aspects of SBOMs and software supply chain security (including reporting and attestation requirements).

The government faces a challenge and an opportunity here to provide the needed harmonization of these rules and regulations to assure an efficient and consistently implemented cyber regime. Coordination could be achieved by further establishing roles and responsibilities for CISA and the Federal Acquisition Security Council (FASC) to manage cybersecurity and supply chain obligations and reporting for federal contractors. This will reduce duplication and overlap in the cybersecurity and software supply chain framework. Such consistency will assure that all stakeholders understand the rules of engagement in the government space and will be able to more easily adjust as those rules evolve to meet the challenges of a dynamic cyber and supply chain environment.

In closing, Chairwoman Mace, Ranking Member Connolly, members of the subcommittee, thank you for the opportunity to appear before you today. I look forward to addressing any questions you might have.