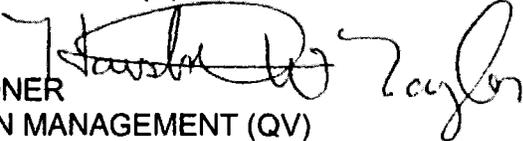




MEMORANDUM FOR JOSEPH NEURAUTER
SENIOR PROCUREMENT EXECUTIVE (SPE)
OFFICE OF ACQUISITION POLICY (V)

FROM: HOUSTON W. TAYLOR 
ASSISTANT COMMISSIONER
OFFICE OF ACQUISITION MANAGEMENT (QV)

SUBJECT: Class Deviation to Federal Acquisition Regulation
(FAR) 8.405-3(a)(6) in Support of the Department of Homeland
Security (DHS) Continuous Diagnostics and Mitigation (CDM)
Program Blanket Purchase Agreements (BPAs)

In accordance with General Services Administration Acquisition Regulation (GSAR) 501.404(a), the Federal Acquisition Service (FAS) requests a class deviation to FAR 8.405-3(a)(6) in support of the DHS CDM program.

FAR 8.405-3(a)(6) permits the establishment of multi-agency BPAs against Federal Supply Schedules contracts if the multi-agency BPAs identify the participating agencies and their estimated requirement at the time the BPAs are established. The requested deviation would permit FAS to establish multi-agency BPAs against Federal Supply contracts without requiring identification of participating agencies and their estimated requirements at the time the BPAs are established. FAS and DHS believe that identifying Federal agencies, state and local, regional, tribal, and other authorized ordering activities and their requirements is not feasible in view of the nature of the CDM program.

The cyber landscape in which our nation operates is a constantly changing and dynamic environment. Threats to information security continue to evolve and government leaders have recognized the need for a modified approach to protect the nation's cyber infrastructure.

To address these concerns, DHS has been given the responsibility to oversee and assist with Government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity solutions within the executive branch per the Office of Management and Budget (OMB) Memorandum 10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the DHS. Memorandum 10-28 grants DHS the primary responsibility within the Executive Branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within the Federal Information Security Management Act of 2002 (FISMA) under 44 U.S.C. §3543. FY13 continuing resolution funds have been provided to DHS for Federal Network Security that may be obligated for operations necessary to establish and sustain essential cybersecurity activities, including procurement and operations of continuous monitoring and diagnostics systems and intrusion detection systems for civilian Federal computer networks.

The CDM initiative is in direct support of the Administration's Cross-Agency Priority (CAP) Goal of Cybersecurity which instructs DHS to lead the Government-wide coordination of efforts related to implementing the continuous monitoring (CM) of Federal information systems, a critical element of a robust information security risk management program per The White House Blog, March 23, 2012. CDM refers to a cybersecurity strategy based on continuous monitoring of Federal networks through the use of sensors. A sensor is typically a software program, usually referred to as a tool, which runs in the background of a computer or other device on the network continually testing for vulnerabilities. The primary goal of continuous monitoring is to transform the otherwise static security assessment and risk mitigation processes into a dynamic program that provides security status through automated data feeds and enables Federal system managers to more effectively and efficiently handle security issues such as missing or misconfigured security controls and to identify suspicious activity.

The CDM program will provide specialized information technology (IT) tools and Continuous Monitoring as a Service (CMaaS) to combat cyber threats in the civilian ".gov" networks. The CDM approach moves away from historical compliance reporting and toward combating threats to the nation's networks on a real time basis. The tools and services delivered through the CDM program will provide Federal agencies with the ability to enhance and automate their existing continuous network monitoring capabilities; correlate and analyze critical security-related information; and enhance risk-based decision making at the agency and Federal enterprise level. Information obtained from the automated monitoring tools will allow for the correlation and analysis of security-related information across the Federal enterprise.

The GSA, FAS, Office of Assisted Acquisition Services (AAS), Federal Systems Integration and Management Center (FEDSIM) intends to award multiple BPAs, on behalf of DHS, for continuous monitoring tools and CMaaS under the solicitation.

It is contemplated that the award of multiple BPAs under the solicitation will be made available for use by all Federal agencies, state and local, regional, tribal, and other authorized ordering activities. A request to authorize state, local, regional, and tribal governments' use of the BPA has been submitted for approval to the FAS Commissioner and it is currently in the approval process.

The CDM program has been unable to fully estimate, and document Federal agencies, state and local, regional, tribal, and other entities complete requirements as required by FAR 8.405-3(a)(6). According to OMB's Fiscal Year (FY) 2011 Federal Information Security Management Act (FISMA) Report to Congress, approximately 78% of Federal agencies have some implementation of CM tools. However, there is not any data which details exactly what the current CM environment is at these agencies. Further complicating this is the fact that many agencies operate CM environments on classified systems. In order to assess the current state of CM for all civilian.gov networks and determine future requirements, DHS would have to conduct an in-depth analysis of each agency within the civilian.gov network. This analysis would be cost-prohibitive and require considerable time and resources from DHS. Nevertheless, in an effort to gather as much information as possible about detailed customer requirements, DHS is currently sending out surveys to prospective customers. The survey will be followed by in-person visits from the DHS CDM to further refine and estimate requirements. DHS currently plans to complete this process before the first BPA order will be awarded.

In the meantime, given the dynamic nature of the cybersecurity environment and continuing attacks that are increasing in number and sophistication, FAS believes it to be in the best interest of the Government to move forward in spite of the lack of complete requirements for all agencies on the basis of the critical need to implement CDM solutions across the civilian.gov networks.

Orders under the BPAs may be placed by GSA, other Federal ordering activities, and state and local, regional, and tribal governments. The orders will provide sufficient information about the agencies, state and local, regional, tribal, and other authorized ordering activities that are expected to participate and their estimated aggregate requirements to enable the quoters to submit definite and meaningful quotes. The BPAs will be established with those Schedule contractors that can provide the IT tools and CMaaS requirements that represent the best value. In order to conduct a valid competition in establishing the BPAs, FAS will use a sample order (SO) in addition to price and requested price reductions. Since the overall BPA-level requirements are unknown and cannot be quantified, the SO will be used as a representative sample of the work that may be required. The use of the SO will provide a common basis for evaluation of technical and management approaches as well as a basis for comparison of price. Five (5) BPAs are contemplated. Participation in the BPAs and resulting task order competitions for non-Federal customers will remain voluntary for Schedule contractors, consistent with the statutory authority in 40 U.S.C. §502 that authorized the Administrator to "provide for the use" of GSA Schedule 70 by state and local governments (defined to include tribal and regional governments).

This deviation request will enable the CDM effort, now and in the future, to recognize and overcome the cybersecurity challenges facing departments and agencies across Government and offer a convenient, economical, and standardized solution set that will help satisfy the requirements of the Administration's CAP Goal of Cybersecurity. The Federal Government will be able to further utilize its economies of scale to order tools and services more efficiently, leverage its buying power, simplify and standardize its continuous monitoring requirements definition, and consequently improve the nation's information system security. Making these CDM BPAs available to state and local, regional, tribal, and other authorized ordering activities will encourage wider use of the solutions and allow these entities to benefit from the same consistency and ease of procurement as will be available to Federal agencies. It is also expected that making the BPAs available to all Federal agencies and other entities will result in reduced pricing and better product offerings from vendors, as a result of a more expansive and standardized customer base. Finally, the Federal Government will be able to further leverage its economy of scale buying power to provide maximum opportunities for small businesses and a mechanism for fast and effective ordering of continuous monitoring solutions.

Based upon the above, FAS requests that a class deviation to FAR 8.405-3(a)(6) be granted for the Continuous Diagnostics and Mitigation, Tools and CMaaS BPAs acquisition.

Should you have any questions regarding this request, please contact Anissa L. Burley, 703-605-9458.



Joseph Neurauter
Senior Procurement Executive
Office of Acquisition Policy (V)

Oct 10, 2012
Date