STATEMENT OF NEED

(141017-25-0038)

PURPOSE: Global Mapper and Global Mapper Pro Network Licenses with Maintenance and Support

SCOPE OR MISSION: The Department of Commerce (DOC), National Oceanic & Atmospheric Administration (NOAA), National Ocean Service's (NOS), Office for Coastal Management (OCM) has a requirement for Global Mapper and Global Mapper Pro Network License network licenses as well as purchase maintenance and support. This software will support lidar elevation data quality assurance analysis and generating public products related to elevation data, sea level rise inundation data, and land cover thematic data.

BACKGROUND: NOAA has long been a leader in lidar elevation data distribution to the public. For many years we have been using Global Mapper as part of our standard processing routine to quickly and efficiently examine the data sets prior to public distribution. It is also an integral part of our digital elevation model creation process for the NOAA Sea Level Rise and Coastal Flooding Impacts viewer. It is likely to be incorporated into the machine learning aspects of the land cover product generation. This purchase will provide updates, maintenance and support for the current version already in use.

TECHNICAL SPECIFICATIONS:

1.) Renewal Global Mapper Network Licenses, 10 concurrent users, qty 10
2.) Renewal Global Mapper Pro Network Licenses, 4 concurrent users, qty 4
3.) Maintenance and Support for licenses listed above under numbers 1 and 2

Must be an authorized Global Mapper reseller and be able to provide proof of authorization.

PERIOD OF PERFORMANCE: To be delivered on or before, May 1, 2025. Contract to include one base period of twelve (12) consecutive months, one option period of twelve (12) consecutive months and a second option period for twenty-four (24) consecutive months.

POINTS OF CONTACT:

Technical:
Kirk Waters, kirk.waters@noaa.gov

Administrative:
Sheri Farrell, Sheri.Farrell@noaa.gov

IT SECURITY REQUIREMENTS:

The Assessment and Authorization (A&A) requirements of Clause 48 CFR 1352.239-72 do not apply, and a Security Accreditation Package is not required.

The following is a list of relevant information the Department of Commerce (DOC) Information Technology (IT) Security takes into consideration when assessing the security requirements and risk for procuring IT products and services.

a) The Contractor shall only supply Information Technology (e.g., hardware, software, firmware, etc.) and/or product license and shall not require the use of any contractor owned equipment. The contractor will not have remote access to any government owned equipment. The Contractor shall ensure the acquiring Information Technology provided disables "phone home" or similar capabilities.

b) Product support and supporting documentation allows for the sanitization of the acquiring Information Technology and/or product license upon the disposal of the product. Product shall allow the use one of the approved methods for secure destruction of data/information including unclassified but sensitive information. Approved methods include NIST Special Publications 800-88 *Guidelines for Media Sanitization* (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf) or the National Security Agency in the *Media Destruction Guidance* (https://www.nsa.gov/Resources/Media-Destruction-Guidance/).

c) The acquiring information technology is engineered for trustworthy and security that is consistent with the engineering-based trustworthy secure solutions as outlined in NIST Special Publication 800-160 Version 1, Revision 1 Engineering Trustworthy Secure Systems (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf) and NIST Special Publication 800-160, Volume 2, Revision 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf).

d) The acquiring information technology complies with Office of Management and Budget Memorandum M-07-18 *Ensuring New Acquisitions Include Common Security Configurations* and the Federal Acquisitions Regulations (FAR) 39.101(d) regulations require NIST common security configuration checklists including United States Government Configuration Baseline (USGCB) initiative. More information is available at National Checklist Program (NCP), (https://nvd.nist.gov/ncp/repository), the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low-level guidance on setting the security configuration of operating systems and applications. The acquiring information technology considers the following requirements:

i. Software procured meets the standard installation, operation, maintenance, updates and/or patching of software shall not alter the configuration settings from the approved USGCB/other secure configuration.

ii. Applications designed for normal end users run in the standard user context without elevated system administration privileges.

iii. Supporting documentation or reference(s) that describes the security capabilities, the design and development processes and the testing and evaluation procedures used by the product or services being provided for this acquisition.

iv. Supporting documentation or reference(s) that describes all product or service updates and enhancements as they are implemented. The product or service supporting documentation could be the user and system administrator guides, which is documents the functional properties of the security controls employed to permit the analysis and testing of the security controls.

e) The acquiring information technology complies with the Homeland Security Presidential Directive 12 (HSPD-12) *Policy for a Common Identification Standard for Federal Employees and Contractors* requirements from FAR 4.1302 stating: (a) In order to comply with Federal Information Processing Standard (FIPS) 201-3 *Personal Identity Verification (PIV) of Federal Employees and Contractors* (https://doi.org/10.6028/NIST.FIPS.201-3), agencies must purchase only approved personal identity verification products and services, (b) Agencies may acquire the approved products and services from the GSA, Federal Supply Schedule 70, Special Item Number (SIN) 132-62, HSPD-12 Product and Service Components, in accordance with ordering procedures outlined in FAR Subpart 8.4.

f) The acquiring information technology complies with Internet Protocol Version 6 (IPv6) requirements from FAR part 11.002 requirements that state the agency Chief Information Officer can waive this requirement provided the acquisition requirements documents the appropriate technical capabilities defined in the USGv6 Profile available in the NIST Special Publication (SP) 500-267 (https://www.nist.gov/programs-projects/usgv6-program) and the corresponding declarations of conformance. To meet this requirement each DOC acquisition of IP protocol technology must express requirements for IPv6 capabilities in terms of the USGv6 Profile (i.e., using the USGV6 Capabilities Check List) and vendors must be required to document their product's support of the requested capabilities through the USGv6 test program (https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1) using the USGv6 Suppliers Declaration of Conformity.