**Remark S400_SY**
**Sentry Program – All Supplier Flowdowns**
**Date: 16 December 2025**

This program's OPSEC requirements specifically state CUI requires US citizens only, not US persons:

- A US citizen is an individual who has obtained citizenship through birth in the US, naturalization, or through US citizen parents.
- A US person includes not only US citizens, but also legal permanent residents (green card holders) and individuals who meet the substantial presence test (those who have been physically present in the US for a certain number of days).
- US citizens with dual citizenship must have customer approval before working on this program.

CUI-controlled build / test area confirmed
Controlled shipping for unique parts incoming and finished units outgoing confirmed
Counterintelligence / Insider Threat management

**(U) Reporting Requirements**
(U) The Seller agrees that, for a period of three (3) years after the completion of this Agreement, all data generated under this agreement, but not delivered to the MPO, must be made available to MPO representatives upon request by the MPO AO or MPO PM.

**(U) Intellectual Property Rights**
(U) All data and Technology generated by Seller under the Agreement shall be owned by Seller.
**(U) Government's Rights**
(U) Seller will provide the Government with Government Purpose data rights in perpetuity in all technical data and software delivered under this Agreement for a period of three (3) years after completion of this Agreement with the following exceptions listed below.
(U) Additional data rights exceptions may be identified after award when based on new information or inadvertent omissions unless the inadvertent omissions would have materially affected the source selection decision.
**(U) Lower Tier Agreements**
(U) The Seller shall include this Article, suitably modified to identify the parties, in any subcontracts, as applicable.
**(U) Marking of Scientific/Technical Data**
(U) All Seller generated data item deliverables (DIDs) containing scientific and/or technical data, as well as, signals intelligence and communications security information must bear the statement "Not Releasable to the Defense Technical Information Center per DoD Directive 3200.12."
(U) In addition to the above marking, all unclassified technical data/reports, photographs, drawings, schematics, design circuits and description of equipment designed and/or produced under the agreement must be marked with the appropriate dissemination control and distribution statement(s) in accordance with the Agency classification marking procedures. Where SF Form 298 is required to accompany a document, the dissemination control and distribution statement(s) must be entered in Block 12a thereof.
(U) The Seller is responsible for inserting the appropriate application date in the aforementioned legend. This date must be the date upon which the document was completed.

**(U) Foreign Access To Technology**
(U) This Article shall remain in effect during the term of the Agreement and for five (5) years thereafter.

**(U) Restrictions on Sale or Transfer of Technology to Foreign Firms or Institutions**

(U) The Agency shall have and retain the absolute right to deny entering into discussions or agreements with any foreign entity concerning the prototype or product. To the extent that any foreign discussions or agreements may be permitted by the Agency, Seller shall comply with all applicable laws and regulations regarding export-controlled items prior to entering into any discussions or agreements concerning the marketing, sale, release, co-production, and/or exchange of the prototype or product equipment or information with, including but not limited to, any foreign person, foreign governments, foreign agencies, foreign companies, or foreign government-authorized users.

**(U) Lower Tier Agreements**

(U) The Seller shall include this Article, suitably modified, to identify the Parties, in all subcontracts or lower tier agreements, regardless of tier, for experimental, developmental, or research work.

**(U) Security Requirements**

**A. (U) Safeguarding Controlled Unclassified Information & Controlled Technical Information and Cyber Incident Reporting**

I. (U) Protection of Controlled Unclassified information (CUI) and Controlled Technical lnformation (CTI) is of paramount importance to MPO and can directly impact the ability of MPO to successfully conduct its mission. Therefore, this Article requires the Seller to protect CUI and CTI that resides on the Seller's information systems. This article also requires the Seller to rapidly report any cyber incident involving CUI or CTI.

2. (U) The Seller shall implement the version of NIST Special Publication (SP) 800-171 in effect at the time the solicitation is issued or as authorized by the MPO Agreements Officer for CUI and CTI that resides on the Seller's information systems. Consistent with NIST SP 800-171, implementation may be tailored to facilitate equivalent safeguarding measures used in the Seller systems and organization. Any suspected loss or compromise of CUI or CTI that resides on the Seller's information systems shall be considered a cyber-incident and require the Seller to rapidly report the incident to MPO in accordance with subparagraph 8.3 of this Article.

3. (U) Upon discovery of a cyber-incident involving CUI or CTI, the Seller shall take immediate steps to mitigate any further loss or compromise. The Seller shall rapidly report the incident to MPO and provide sufficient details of the event-including identification of detected and isolated malicious software-to enable MPO to assess the situation and provide feedback to the Seller regarding further reporting and potential mitigation actions. The Seller shall preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days from reporting the cyber incident to enable MPO to assess the cyber incident. The Seller agrees to rapidly implement security measures as recommended by MPO and to provide to MPO any additionally requested information to help the Parties resolve the cyber incident and to prevent future cyber incidents.

4. (U) All information and data covered by this Article must be reviewed and approved by MPO prior to any public release, with requests routed through the Government's points of contacts identified herein.

5. (U) The Seller shall include this Article in all subcontracts or lower tier agreements, regardless of tier, for work performed in support of this Agreement.

**B. {U) Adequate Security**

(U) The Seller shall provide adequate security on all covered Seller information systems. To provide adequate security, the Seller shall implement, at a minimum, the following information security protections:

(U) For covered Seller information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

• Cloud computing services shall be subject to the security requirements specified in 48 CFR 239.7602,
• Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this agreement.
(U) For covered Seller information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified above the following security requirements apply:
(U) The covered Seller information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at https:l/csrc.nist.govlpublicationslspB00) in effect at the time the solicitation is issued or as authorized by the Agreements Officer.
(U) The Seller shall submit requests to vary from NIST SP 800-171 in writing to the Agreements Officer, for consideration by the DoD CIO. The Seller need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.
(U) If the DoD CIO has previously adjudicated the Seller's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Agreements Officer when requesting its recognition under this agreement.
If the Seller intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this agreement, the Seller shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https:/lwwwjedramp.govldocuments-temp/ates/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this article for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.
(U) Apply other information systems security measures when the Seller reasonably determines that information systems security measures, in addition to those identified in paragraphs (b){I) and (2) of this article, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

**C. (U) Cyber Incident Reporting**

(U) When the Seller discovers a cyber incident that affects a covered Seller information system or the covered defense information residing therein, or that affects the Seller's ability to perform the requirements of the agreement that are designated as operationally critical support and identified in the agreement, the Seller shall-
• (U) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered Seller information system(s) that were part of the cyber incident, as well as other information systems on the Seller's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Seller's ability to provide operationally critical support; and
• (U//FOUO) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.
(U//FOUO) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.
(U//FOUO) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this article, the Seller or subcontractor shall have or acquire a DoD-approved medium assurance

certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

**D. (U) Malicious Software**

(U) When the Seller or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Agreements Officer. Do not send the malicious software to the Agreements Officer.

**E. (U) Media Preservation and Protection**

(U) When a Seller discovers a cyber-incident has occurred, the Seller shall preserve and protect images of all known affected information systems identified Cyber Incident Reporting section of this article and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

**F. (U) Cyber Incident Damage Assessment Activities**

(U) If DoD elects to conduct a damage assessment, the Agreements Officer will request that the Seller provide all of the damage assessment information gathered in accordance with Media Preservation and Protection paragraph of this article.

**G. (U) DoD Safeguarding and Use of Seller Attributional/Proprietary Information**

(U) The Government shall protect against the unauthorized use or release of information obtained from the Seller (or derived from information obtained from the Seller) under this article that includes Seller attributional/proprietary information, including such information submitted in accordance with Cyber Incident Reporting. To the maximum extent practicable, the Seller shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the Seller attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

**H. (U) Use and Release of Seller Attributional/Proprietary Information not created by or For DoD**

(U) Information that is obtained from the Seller ( or derived from information obtained from the Seller) under this article that is not created by or for DoD is authorized to be released outside of DoD-

- To entities with missions that may be affected by such information;
- To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
- To Government entities that conduct counterintelligence or law enforcement investigations;
- For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) Sellers in the program at 32 CFR part 236); or
- To a support services Seller ("recipient") that is directly supporting Government activities under an agreement that includes a provision outlining the limitations on the use or disclosure of third-party contractor reported cyber incident information.

**I. (U) Use and Release of Seller Attributional/Proprietary Information created by or for DoD**

(U) Information that is obtained from the Seller ( or derived from information obtained from the Seller) under this article that is created by or for DoD (including the information submitted pursuant to Cyber Incident Reporting) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph I of this article, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

**J. (U) Disclosure of Electronic Communications Data**

(U) The Seller shall conduct activities under this article in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

**K. (U) Other Safeguarding or Reporting Requirements**

(U) The safeguarding and cyber incident reporting required by this article in no way abrogates the Seller's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable articles of this agreement, or as a result of other applicable U.S. Government statutory or regulatory requirements.

**L. (U) Subcontracts**

(U) The Seller shall-

Include this article, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Seller shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this article, and, if necessary, consult with the Agreements Officer; and

(U) Require subcontractors to--

- Notify the prime Seller (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Agreements Officer; and
- Provide the incident report number, automatically assigned by DoD, to the prime Seller ( or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in this article.

**M. (U) Public Release or Dissemination of Information Generally**

(U) The Seller shall not release to anyone outside the Seller's organization any unclassified information, regardless of medium, pertaining to any part of this Agreement or any program related to this Agreement unless the AO has given prior written approval or the information is otherwise in the public domain before the date of release. The Seller must not disclose any information concerning the sponsorship of this Agreement, or the nature of the Government's interest in and application of the subject matter of this Agreement unless this type of information is expressly allowed to be disclosed by written approval of the AO. The Seller agrees to include a similar requirement in each subcontract under this Agreement. Subcontractors shall submit requests for authorization to release information through the Seller to the AO.

**N. (U) Software Requirement**

(U) The Seller warrants that, to the best of its knowledge and belief, software provided under this agreement does not contain any malicious code, program, or other internal component ( e.g., computer virus) which could damage, destroy, or alter software, firmware, or hardware or which could reveal any data or other information accessed through or processed by the software. Further, the Seller must immediately inform the Agreements Officer upon reasonable suspicion that any software provided hereunder may cause the harm described above.

**(U) Prohibition on Contracting for Certain Telecommunications & Video Surveillance Services or Equipment**

**A. (U) Prohibitions**

1. (U) Section 889(a)(l)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract/agreement to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Seller is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this article

applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

2. (U) Section 889(a)(l)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 20 l9 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract/agreement, or extending or renewing a contract/agreement, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph ( c) of this article applies or the covered telecommunication equipment or services are covered by a waiver described in 48 C.F.R. § 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract/agreement.

**B. (U) Exceptions**

(U) This Article does not prohibit the Seller from providing a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements.

**C. (U) Reporting Requirement**

1. (U//FOUO) In the event the Seller identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during agreement performance, or the Seller is notified of such by a subcontractor at any tier or by any other source, the Seller shall report the information in paragraph ( d)(2) of this article to the Agreement Officer, unless elsewhere in this agreement are established procedures for reporting the information; in the case of the Department of Defense, the Seller shall report to the website at https://dibnet.dod.mil.

2. (U) The Seller shall report the following information pursuant to subparagraph D. I. of this Article:

a. Within one business day from the date of such identification or notification: The agreement number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

b. Within 10 business days of submitting the information in paragraph ( d)(2)(i) of this article: Any further available information about mitigation actions undertaken or recommended. In addition, the Seller shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

**D. (U) Subcontracts**

(U) The Seller shall insert the substance of this article, including this paragraph E, in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

**(U) Prohibition on Contracting For Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities**

**A. (U) Prohibition**

(U) Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any Kaspersky Lab covered article. The Seller is prohibited from-

( I) Providing any Kaspersky Lab covered article that the Government will use on or after October I, 2018; and

(2) Using any Kaspersky Lab covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the agreement.

**B. (U) Reporting requirement**

(U//FOUO) (1) In the event the Seller identifies a Kaspersky Lab covered article provided to the Government during agreement performance, or the Seller is notified of such by a subcontractor at any tier or any other source, the Seller shall report, in writing, to the Agreement Officer or, in the case of the Department of Defense, to the website at https://dibnet.dod.mil.

(U) (2) The Seller shall report the following information pursuant to paragraph (c)(l) of this article:

(i) Within 3 business days from the date of such identification or notification: the agreement number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph ( c )(I) of this article: any further available information about mitigation actions undertaken or recommended. In addition, the Seller shall describe the efforts it undertook to prevent use or submission of a Kaspersky Lab covered article, any reasons that led to the use or submission of the Kaspersky Lab covered article, and any additional efforts that will be incorporated to prevent future use or submission of Kaspersky Lab covered articles.

**C. (U) Subcontracts.**

(U) The Seller shall insert the substance of this article, including this paragraph (d), in all subcontracts including subcontracts for the acquisition of commercial products or commercial services.

**(U) Taxes, Tariffs, Duties, and Importation Costs**

(U) This language has not yet been finalized, but will be flowed to Lower Tier Subcontractors in the very near future.