



Solicitation # CJ18012

Attachment S

Wireless Data, Voice and Accessories RFP

Security Disclosure Statement

---

- A. Purchasing entities are concerned about the security and privacy of information and data related to the performance of this contract. The type of data and information transmitted, stored and processed by the products and services will vary based on the purchasing entities requirements. As a result, it is not possible to establish a single set of security requirements all products and services awarded under this contract must meet. Each purchasing entity purchasing from this contract will determine which products and services have the appropriate cyber security and data controls in place to meet their specific needs. To assist public entities each offeror must submit a Security Disclosure Statement with their proposal.
- B. To qualify for any award under this contract, the Offeror must submit a Security Disclosure Statement addressing all of the elements listed below.
  - i. In responding, Offeror must address not only the security mechanisms used by the bidder and its direct subsidiaries, but any partners, subcontractors or other 3<sup>rd</sup> parties who would be involved in implementing, operating, or in any way coming into contact with the service.
  - ii. By signature of the proposal submitted in response to this RFP, the offeror represents and warrants the accuracy and currency of the information submitted in response to the Security Disclosure Statement as listed in paragraph C of this attachment.
- C. Security Disclosure Statement information required. Offeror shall describe all policies, procedures, measures, methods, certifications and standards the offered product and/or service has in place to protect the purchasing entities security and privacy of information and data involved in the performance of this contract for each numbered statement below. Description responses shall also include;

- i. If for the specific product or service offered, the numbered security statement is not appropriate because it does not as a matter of accepted security practice relate to the product or service offered, the offeror shall indicate in a statement that it is not applicable and briefly explain why.
  - ii. If the specific product or service offered does not comply with the the numbered statement, the offer shall indicate, “does not comply”.
- 
- 1) Methods and measures taken to hold, protect, and dispose of data during and following completion of any contract services. Include how access to a Purchasing Entity’s user accounts or data will not be allowed, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.
  - 2) Security measures to secure and protect the confidentiality of information and data that is obtained, created, stored, transmitted, processed or otherwise held or managed by the product or service during the performance of all work related to performance of this contract. Include all data confidentiality standards and practices that prevent the exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data.
  - 3) Data encryption methods and standards in place to encrypt data at rest and in transit. This includes but is not limited to, encryption standards employed to protect data in transit over either wired or wireless (e.g. cellular, Wi-Fi, or other), and how that might change over the life of the contract.
  - 4) Measures to protect Information about the cost, type, quantity and location of state communications facilities, system assets, plans, procedures, contract information, billing information and other information identified as sensitive by the purchasing entity related to the performance of all work under this contract.
  - 5) Risk and policy management and enforcement measures in place to protect the security of physical assets and information.
  - 6) How distributed access is controlled and managed across IT assets, including data, applications, networks and platforms within the solution.
  - 7) Security management in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.
  - 8) Describe the logging process including:
    - a. The types of services and devices logged,
    - b. The event types logged, and
    - c. The information fields will be made available to the authorized Purchasing Entity if requested in their PA after award of the master agreement.

- 9) Describe the security Technical Reference Architectures
- 10) Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offerors employees who have access to sensitive data.
- 11) Provide an itemized list of all cyber security standards and, security certifications in place that the products and service offered comply with to ensure appropriate controls and data confidentiality are in place, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800- 171, FIPS 200 and FedRAMP (Moderate, High) if they apply. Include detailed response on how security standards and certifications will be maintained and updated to meet best practices for maintenance and operations.
- 12) Provide a detailed list of all third-party attestations, security credentials and certifications, and reports relating to data security, integrity, and other controls in place.
- 13) NIST Cybersecurity Framework, April 16, 2018, Version 1.1  
<https://doi.org/10.6028/NIST.CSWP.04162018>: Describe how the offeror is prepared to utilize the NIST Cybersecurity Framework for Turnkey Internet of Things, Other Turnkey Wireless, Applications and Services (Category 3) and Wireless Transport Options (Category 4) as may be implemented by the Purchasing Entity, which may include, but is not limited to:
  - a. Convey the purchasing entities' cyber security requirements,
  - b. Identify Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities will provide in the Offerors's system, products or services under contract with the Purchasing Entity,
  - c. Communicate cyber security requirements through Cyber Supply Chain Risk Management (SCRM), and
  - d. Other cybersecurity risk management activities of Offeror's system, products or services under contract with the purchasing entity.
- 14) NIST Cybersecurity Framework, Table 2 Framework Core: For each subcategory of the all 15 Categories of the NIST Cybersecurity Framework, list the specific standards and certifications, the products or services offered comply with at the time or your proposal. Categories Include:
  - a. Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

- b. Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- c. Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- d. Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- e. Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- f. Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
- g. Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- h. Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.
- i. Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- j. Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- k. Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

- l. Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
- m. Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
- n. Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
- o. Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
- p. Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
- q. Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
- r. Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
- s. Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
- t. Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
- u. Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
- v. Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
- w. Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

- 15) Describe the data breach/incident policies and procedures regarding notification to both the purchasing entity of a security incident and/or data breach, as defined in this RFP, and the mitigation of such a breach. Include how proposer will work with Purchasing Entities before, during, and after a Security Incident and a Data Breach. Include information such as:
- a. Personnel who will be involved at various stages, include detail on how the Contract Manager will be involved;
  - b. Response times;
  - c. Incident levels;

- d. Processes and timelines;
- e. Methods of communication and assistance; and
- f. Other information vital to understanding the service you provide.

Provider should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

16) Describe the method for compliance with all applicable laws related to data privacy and security including state Security Breach Notification Laws dealing with personally identifiable information (PII). Describe any legal obligations related to security the offeror will meet over the life of the contract and describe how offeror will report changes to these obligations to the public entity.

- D. Any Turnkey Internet of Things, Other Turnkey Wireless system that incorporates SaaS, IaaS or PaaS or other cloud computing element shall complete, provide, and maintain a completed CSA STAR Registry Self-Assessment for that element. 2 < [https://cloudsecurityalliance.org/star/self-assessment/#\\_overview](https://cloudsecurityalliance.org/star/self-assessment/#_overview) . Offeror must either submit a completed Consensus Assessments Initiative Questionnaire (CAIQ), or submit a report documenting compliance with Cloud Controls Matrix (CCM) that the CAIQ is based on for the element that cloud based.