**General Services Administration**  
**Federal Supply Service Authorized Federal Supply Schedule Price List**

<table>
<thead>
<tr>
<th>SIN 518210C Cloud and Cloud-Related IT Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly Adaptive Cybersecurity Services – HACS – SIN 54151HACS</td>
</tr>
</tbody>
</table>

- **High Value Asset (HVA) Assessment** – evaluate a subset of the agency's HVA security posture and identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities.

- **Risk and Vulnerability Assessment** – RVA – conduct assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

- **Cyber Hunt** activities are responses to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.

- **Incident Response** services help organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.

- **Penetration Testing** is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

<table>
<thead>
<tr>
<th>SIN 54151S Information Technology Professional Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIN OLM Order-Level Materials</td>
</tr>
</tbody>
</table>

**Schedule Title:** Multiple Award Schedule (MAS)

- **PSC Class DA10:** IT and Telecom – Business Application/Application Development Software as a Service
- **PSC Class DD01:** IT and Telecom – Service Delivery Support Service: ITSM, Operations Center, Project/PM (Labor)
- **PSC Class DJ01:** IT and Telecom – Security and Compliance Support Services (Labor)
- **PSC Class DJ10:** IT and Telecom – Security and Compliance as a Service
- **PSC Class R499:** Support – Professional: Other
- **PSC Class R704:** Support – Management: Auditing
- **PSC Class R799:** Support – Management: Other

**Contract No.:**  
GS-35F-399DA

**Contract Period:**  
07/07/2016–07/06/2026

---

**TalaTek**  
12026 Hamden Court  
Oakton, VA 22124-2207  
Attn: Baan Alsinawi  
Tel: 571-771-0071  
www.talatek.com

**Business size:** Small

---

**Federal Supply Service Multiple Award Schedule**

- **Pricelist current through Modification #:**  
Original contract, dated 07/07/2016,  
Mod No. PA-0026, effective 08/29/2022, and  
Mass Mod A847, accepted 07/05/2022.

- **Prices Shown Herein are Net** (discount deducted)

- **On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order is available through GSA Advantage®, a menu-driven database system. The INTERNET address for GSA Advantage® is:**  
https://gsaadvantage.gov/

- **For more information on ordering from Multiple Award Schedules, please visit**  
https://www.gsa.gov/schedules.
Customer Information

1. Special Item Numbers (SINs) and Labor Rates
   a. Table of Awarded Special Item Numbers (SINs)

<table>
<thead>
<tr>
<th>SIN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIN 518210C</td>
<td>Cloud and Cloud-Related IT Professional Services</td>
</tr>
<tr>
<td>SIN 54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>SIN 54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>SIN OLM</td>
<td>Order-Level Materials</td>
</tr>
</tbody>
</table>

b. TalaTek intelligent Governance and Risk Integrated Solution (TiGRIS) FISMA & FedRAMP Continuous Monitoring (ConMon) Software-as-a-Solution (SaaS)

With the TalaTek intelligent Governance and Risk Integrated Solution (TiGRIS), FedRAMP accredited, managed service, you do not need to be an expert in Compliance. TiGRIS is preconfigured with a variety of frameworks to meet your business needs, predefined workflows, risk metrics, dashboards, and reports. We provide what is needed to get your program up and going quickly. TiGRIS supports multiple standards such as FISMA and FedRAMP (NIST 800-53), NIST Cybersecurity Framework (CSF), and other standards. We help your organization gain control over and visibility into the complex security requirements, deliverables, and ongoing risk management tasks. With customizable Risk Scoring tailored to your unique risk appetite and mapped to your system specific, inherited, and hybrid security controls, TiGRIS is designed to help determine your residual risks. Automated workflows and Alerts ensure compliance tasks are completed on time. A centralized Evidence Library serves as a one-stop-shop for all artifacts and documentation. If your organization already has its compliance team and processes established and you’re looking for a better way to manage and automate the process, TalaTek's public offering is for you. However, if you would like TalaTek's experts to guide you through the complexities of the various frameworks and standards, please contact us about our private offerings.

<table>
<thead>
<tr>
<th>Unit</th>
<th>Description</th>
<th>Rate (USD/Month) including IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Package</td>
<td>TiGRIS FISMA Continuous Monitoring SaaS (1-5 Systems)</td>
<td>$1,974.81</td>
</tr>
<tr>
<td>FISMA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Package</td>
<td>TiGRIS FedRAMP ConMon SaaS (1-5 Systems)</td>
<td>$2,468.51</td>
</tr>
<tr>
<td>FedRAMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Package</td>
<td>TiGRIS Cyber Security Framework (CSF) SaaS (1-5 Systems)</td>
<td>$987.41</td>
</tr>
<tr>
<td>Secure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO17020</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
c. TalaTek Labor Rate Pricelist

<table>
<thead>
<tr>
<th>CLIN</th>
<th>Labor Category</th>
<th>Rate (USD/Hour) including IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>54151S Information Technology Professional Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTK-01.2</td>
<td>Technical Writer</td>
<td>$101.58</td>
</tr>
<tr>
<td>TTK-02.2</td>
<td>Project Manager</td>
<td>$128.36</td>
</tr>
<tr>
<td>TTK-02.3</td>
<td>Program Manager</td>
<td>$172.79</td>
</tr>
<tr>
<td>TTK-03.2</td>
<td>Deputy Quality System Manager</td>
<td>$133.30</td>
</tr>
<tr>
<td>TTK-03.3</td>
<td>Quality System Manager</td>
<td>$153.05</td>
</tr>
<tr>
<td>TTK-04.3</td>
<td>Senior Information Security Consultant</td>
<td>$246.85</td>
</tr>
<tr>
<td>TTK-05.1</td>
<td>Junior Continuous Monitoring Analyst</td>
<td>$93.80</td>
</tr>
<tr>
<td>TTK-05.2</td>
<td>Continuous Monitoring Analyst</td>
<td>$133.30</td>
</tr>
<tr>
<td>TTK-05.3</td>
<td>Senior Continuous Monitoring Analyst</td>
<td>$172.80</td>
</tr>
<tr>
<td><strong>518210C Cloud and Cloud-Related IT Professional Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTK-11.2</td>
<td>Cloud Services Technical Writer</td>
<td>$101.58</td>
</tr>
<tr>
<td>TTK-12.2</td>
<td>Cloud Services Project Manager</td>
<td>$128.36</td>
</tr>
<tr>
<td>TTK-13.1</td>
<td>Junior Cloud Continuous Monitoring Analyst</td>
<td>$93.80</td>
</tr>
<tr>
<td>TTK-13.2</td>
<td>Cloud Continuous Monitoring Analyst</td>
<td>$133.29</td>
</tr>
<tr>
<td>TTK-13.3</td>
<td>Senior Cloud Continuous Monitoring Analyst</td>
<td>$172.79</td>
</tr>
<tr>
<td><strong>54151HACS Highly Adaptive Cybersecurity Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTK-21.2</td>
<td>Cybersecurity Technical Writer</td>
<td>$101.58</td>
</tr>
<tr>
<td>TTK-22.2</td>
<td>Cybersecurity Project Manager</td>
<td>$128.36</td>
</tr>
<tr>
<td>TTK-22.3</td>
<td>Cybersecurity Program Manager</td>
<td>$172.79</td>
</tr>
<tr>
<td>TTK-23.2</td>
<td>Deputy Cybersecurity Quality System Manager</td>
<td>$133.29</td>
</tr>
<tr>
<td>TTK-23.3</td>
<td>Cybersecurity Quality System Manager</td>
<td>$153.04</td>
</tr>
<tr>
<td>TTK-24.3</td>
<td>Senior Information Cybersecurity Consultant</td>
<td>$246.85</td>
</tr>
<tr>
<td>TTK-25.1</td>
<td>Junior Cybersecurity Continuous Monitoring Analyst</td>
<td>$93.80</td>
</tr>
<tr>
<td>TTK-25.2</td>
<td>Cybersecurity Continuous Monitoring Analyst</td>
<td>$133.29</td>
</tr>
<tr>
<td>TTK-25.3</td>
<td>Senior Cybersecurity Continuous Monitoring Analyst</td>
<td>$172.79</td>
</tr>
<tr>
<td>TTK-26.2</td>
<td>Cybersecurity Analyst</td>
<td>$133.30</td>
</tr>
<tr>
<td>TTK-26.3</td>
<td>Senior Cybersecurity Analyst</td>
<td>$153.05</td>
</tr>
<tr>
<td>TTK-27.2</td>
<td>Information Cybersecurity Analyst</td>
<td>$123.42</td>
</tr>
<tr>
<td>TTK-27.3</td>
<td>Senior Information Cybersecurity Analyst</td>
<td>$143.17</td>
</tr>
<tr>
<td>TTK-28.2</td>
<td>Cybersecurity Control Assessor</td>
<td>$138.23</td>
</tr>
<tr>
<td>CLIN</td>
<td>Labor Category</td>
<td>Rate (USD/Hour) including IFF</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>TTK-29.1</td>
<td>Junior Cybersecurity Vulnerability Analyst</td>
<td>$93.80</td>
</tr>
<tr>
<td>TTK-30.1</td>
<td>3PAO Junior Cybersecurity Assessor</td>
<td>$140.21</td>
</tr>
<tr>
<td>TTK-30.2</td>
<td>3PAO Cybersecurity Penetration Tester</td>
<td>$182.67</td>
</tr>
<tr>
<td>TTK-30.3</td>
<td>3PAO Senior Cybersecurity Assessor</td>
<td>$182.67</td>
</tr>
<tr>
<td>TTK-31.3</td>
<td>Virtual Chief Information Security Officer - Cybersecurity</td>
<td>$192.54</td>
</tr>
</tbody>
</table>

A description of TalaTek Labor Categories is listed at the end of this pricelist.
2. **Maximum Order***:
   - SIN 518210C: $500,000/per Order
   - SIN 54151HACS: $500,000/per Order
   - SIN 54151S: $500,000/per Order
   - SIN OLM: $250,000/per Order

   *If the best value selection places your order over the Maximum Order identified in this catalog/price list, you have an opportunity to obtain a better schedule contract price. Before placing your order, contact the aforementioned contractor for a better price. The contractor may: (1) offer a new price for this requirement, (2) offer the lowest price available under this contract, or (3) decline the order.

   A delivery order that exceeds the Maximum Order may be placed under the schedule contract in accordance with FAR 8.404.

3. **Minimum Order**: $100

4. **Geographic Coverage**:
   - 518210C: Worldwide
   - 54151HACS and 54151S: Domestic delivery within the 48 contiguous states; Alaska; Hawaii; Puerto Rico; Washington, DC; and U.S. Territories. Note that for products, domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

5. **Point(s) of Production**: N/A – Services Only

6. **Discount from List Prices**: Prices shown are GSA net prices.

7. **Quantity/Volume Discount**: 1% additional discount for labor costs greater than $1,000,000. Reimbursable costs, such as Travel or Other Direct Costs, are not included in the volume discount offered.

8. **Prompt Payment Terms**: None

   **Information for Ordering Offices**: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9. **Foreign Items**: N/A

10. **Delivery**
    a. **Time of Delivery**: Negotiated at Task Order Level
    b. **Expedited Delivery**: Negotiated at Task Order Level
       - Items available for expedited delivery are noted in this price list.
       - Note: All labor categories are available for negotiated expedited delivery.
    c. **Overnight and 2-day Delivery**: Negotiated at Task Order Level
    d. **Urgent Requirements**: Agencies can contact the Contractor’s representative to affect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.

11. **FOB Point**: Destination

    Note: All travel required in the performance of this contract and orders placed hereunder must comply with the Federal Travel Regulations (FTR) or Joint Travel Regulations (JTR), as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all contractor travel. Contractors cannot use GSA city pair contracts. The contractor shall not add the Industrial Funding Fee onto travel costs.
12. **Ordering**
   a. **Ordering Address**: Same as Contractor’s address.
   b. **Ordering Procedures**: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs) are found in Federal Acquisition Regulation (FAR) 8.405-3.

13. **Payment Address**: Same as Contractor’s address.

14. **Warranty Provision**: Standard Commercial Warranty. Customers should contact the contractor for a copy of the warranty.

15. **Export Packing Charges**: N/A

16. **Terms and Conditions of Rental, Maintenance, and Repair (if applicable)**: N/A

17. **Terms and Conditions of Installation (if applicable)**: N/A

18. **Other Terms and Conditions**
   a. **Terms and Conditions of Repair Parts Indicating Date of Parts Price Lists and any Discounts from List Prices (if applicable)**: N/A
   b. **Terms and Conditions for any Other Services (if applicable)**: N/A

19. **List of Service and Distribution Points (if applicable)**: N/A

20. **List of Participating Dealers (if applicable)**: N/A

21. **Preventive Maintenance (if applicable)**: N/A

22. **Special Attributes**
   a. **Special Attributes such as Environmental Attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants)**: N/A
   b. **Section 508 Compliance for EIT**: N/A

23. **Unique Entity Identifier (UEI) Number**
   a. **DUNS Number**: 784575875
   b. **SAM Unique ID**: WN1UKHV49AC4

24. **Notification regarding registration in System for Award Management (SAM) database**: Contractor is registered and valid in SAM until 11/12/2022.
TiGRIS END USER LICENSE AGREEMENT

TERMS AND CONDITIONS

This End User License Agreement (“Agreement”) is entered into effective as of ____ 20xx ("Effective Date") by and between TalaTek ("LICENSOR" or "VENDOR"), a Virginia company located at 12026 Hamden Court, Suite 101, Oakton, VA 22124 and an Ordering Activity (an entity entitled to order under the GSA Schedule contracts as defined in GSA Order ADM 4800.2I, as may be revised from time to time) ("LICENSEE" or "CLIENT").

WHEREAS, LICENSOR is the owner of a certain commercial computer software technology platform called "TiGRIS", that provides a risk management and compliance solution that is provided as a service to LICENSOR’S authorized licensees (the "TiGRIS Software"); and

WHEREAS, LICENSEE desires to obtain from LICENSOR, and LICENSOR desires to provide to LICENSEE, a non-exclusive license to access and use the TiGRIS Software for LICENSEE’s own internal use under the terms and conditions more fully set forth herein, and to receive certain data from use of the TiGRIS Software; and

WHEREAS, in connection with the TiGRIS Software, Licensor will provide certain related services (the “Services”) as set forth in the related purchase order (the “PO”); and

This License Agreement is incorporated by reference into and includes all of the terms of the PO between Client and TalaTek (collectively, the "Agreement"). In consideration of the foregoing recitals, which are hereby made a part of this Agreement, and the terms and conditions specified herein, the parties hereto agree as follows by signature of the PO:

1. **License Grant.** LICENSOR hereby grants to LICENSEE, subject to all of the terms and conditions of this Agreement, and all rights required under 48 CFR § 27.405-3, and 48 CFR § 52.227-19, a non-exclusive, non-transferable, non-sublicensable limited license, to access the TiGRIS Software solely for internal purposes in accordance with this Agreement and the user documentation associated with the TiGRIS Software. The rights set forth in this paragraph apply notwithstanding any other provisions herein.

2. **License Terms.** LICENSEE will not, directly or indirectly, (i) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the TiGRIS Software; (ii) modify, translate, copy, or create derivative works based on the TiGRIS Software; (iii) rent, lease, distribute, sell, resell, assign, or otherwise transfer rights to the TiGRIS Software; (iv) remove any proprietary notices from the TiGRIS Software; (v) publish or disclose to third parties any evaluation of the TiGRIS Software without LICENSOR’s prior written consent; or (vi) create any link to the TiGRIS Software or frame or mirror any content contained on, or accessible from, the TiGRIS Software.

   a. Notwithstanding any contrary provisions contained in this Agreement, the Licensor agrees that the Licensee will have the rights that are set forth in paragraph (b) of this clause to use, duplicate or disclose any commercial computer software delivered under this contract. The terms and provisions of this contract shall comply with Federal laws and the Federal Acquisition Regulation.

   b. (1) The commercial computer software delivered under this contract may not be used, reproduced, or disclosed by the Licensee except as provided in this clause or as expressly stated otherwise in this contract.

      (2) If the commercial computer software is otherwise available without disclosure restrictions, the Licensor licenses it to the Licensee without disclosure restrictions.
(3) The Licensor shall affix a notice substantially as follows to any commercial computer software delivered under this contract.

(4) Notice-Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Licensee regarding its use, and disclosure are limited as may be set forth in any applicable Federal Acquisition Regulations or under an applicable government contract under which the TiGRIS Software is separately provided.

3. Payment and Payment Terms. LICENSEE will pay LICENSOR the fees as outlined in the Schedule contract/PO for this License. Licensee will reimburse VENDOR for reasonable out-of-pocket expenses incurred in the performance of Services only if specifically authorized on the applicable PO and Schedule contract. Vendor agrees to maintain appropriate records and to submit copies of all receipts necessary to support such expenses at the intervals and in the manner prescribed by Client. Any addition to or modification of the Services to be provided by VENDOR must be set forth in a written amendment to the PO, including but not limited to, additional subcontractor service agreements, special projects, and additional labor or materials. Any such amendments must be mutually agreed and when executed, shall become a part of this Agreement and subject to its terms and conditions.

4. Term and Termination. This Agreement has a term and subscription start date as outlined in the PO. This Agreement may be terminated in accordance with FAR 52.212-4(l), FAR 52.212-4(m), and GSAR 552.238-73. This license terminates upon termination of the Agreement or term.

5. Ownership of Software and Data. All right, title, ownership and interest in and to the TiGRIS software (for engagements that have agreed to utilize the TiGRIS software), and any data and documentation provided by LICENSOR and/or any other manufacturers (such as manuals, guides, and product descriptions and specifications), shall remain with LICENSOR, or to other manufacturers, as appropriate. LICENSEE warrants and agrees that it will not reverse engineer any products or source code provided in connection with this Agreement. All documents, data, and other information belonging to LICENSEE shall remain the property of LICENSEE. LICENSEE shall accordingly own, and remain responsible for, all private and personal information within LICENSEE’S database and/or platform, including all information belonging to LICENSEE, LICENSEE’S customers, employees, or other persons. LICENSEE’S database, and documentation serviced by LICENSOR may include source code and/or other intellectual property belonging to Licensee and/or third parties. Notwithstanding the foregoing, LICENSEE shall have the rights set forth in Section 1 of this Agreement, above.


a. LICENSEE acknowledges that LICENSOR is the owner of all intellectual property rights (including the copyrights) in the TiGRIS Software (other than intellectual property provided by LICENSOR), and that material published by LICENSOR in connection with the TiGRIS Software may contain other proprietary notices or describe products, software, processes or technologies owned by LICENSOR or third parties. LICENSEE acknowledges that nothing in this Agreement or in the TiGRIS Software shall be construed as granting to LICENSEE a license to any copyright, trademark, patent or other intellectual property right of LICENSOR or any third party, except as expressly set forth herein.

b. LICENSEE acknowledges that certain brand names or logos and the “look” and “feel” of the TiGRIS Software (including color combinations, button shapes, layout, design and all
other graphic elements) are trademarks or copyrights of LICENSOR. All related product or service names, design marks and slogans are the trademarks or service marks of LICENSOR. All other product and service marks contained on the TiGRIS Software are the trademarks or service marks of LICENSOR or third parties. The deletion or alteration of any copyright or other proprietary notices from the TiGRIS Software by LICENSEE, its agents or any third party is strictly prohibited.

c. LICENSEE acknowledges that all editorial content and graphics used in connection with the TiGRIS Software, all HTML-based computer programs used to generate pages and any and all manuals and technical guides are protected by U.S. copyright laws and international treaties and may not be copied without the prior written consent of LICENSOR or LICENSOR as the applicable owner thereof, each of which reserves all rights. Use or re-use of any editorial content and graphics for any purpose is strictly prohibited.

7. Remedies, Disclaimers & Limitations.

a. LICENSEE assumes all responsibility and risk for LICENSEE’s use of the TiGRIS Software and the Internet generally.

b. LICENSEE EXPRESSLY AGREES THAT THE USE OF THE TIGRIS SOFTWARE IS AT THE LICENSEE’S SOLE RISK. THE TIGRIS SOFTWARE, AND ALL CONTENTS OF THE FOREGOING ARE PROVIDED TO LICENSEE ON AN “AS IS” AND “AS AVAILABLE” BASIS BY LICENSOR. LICENSOR EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF TITLE, NONINFRINGEMENT, ALL WARRANTIES ARISING BY USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE, AND IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. LICENSOR MAKES NO WARRANTY THAT THE TIGRIS SOFTWARE WILL MEET LICENSEE’S REQUIREMENTS, OR THAT THE INFORMATION ON THE TIGRIS SOFTWARE, REPORTS, TOOLS, APPLICATIONS OR THE INTERNET GENERALLY WILL BE UNINTERRUPTIBLE OR ERROR FREE OR THAT ANY INFORMATION, SOFTWARE OR OTHER MATERIAL ACCESSIBLE FROM THE TIGRIS SOFTWARE IS FREE OF VIRUS OR OTHER HARMFUL COMPONENTS. LICENSOR MAKES NO WARRANTY AS TO THE ACCURACY OR RELIABILITY OF THE TIGRIS SOFTWARE. LICENSEE ACKNOWLEDGES AND AGREES THAT ANY MATERIAL DATA DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE TIGRIS SOFTWARE IS DONE AT LICENSEE’S OWN DISCRETION AND RISK, AND THAT LICENSEE WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO LICENSEE OR ITS COMPUTER SYSTEM THAT RESULT. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, SO SOME OF THE ABOVE EXCLUSIONS MAY NOT APPLY TO LICENSEE. This clause does not limit or disclaim any of the warranties specified in the GSA MAS Schedule contract under FAR 52.212-4(o). In the event of a breach of warranty, the U.S. Government reserves all rights and remedies under the contract, the Federal Acquisition Regulations, and the Contract Disputes Act, 41 U.S.C. 7101-7109.

c. No advice or information given by LICENSOR, its affiliates or their respective employees shall modify the foregoing or create any warranty.

EXCEPT AS OTHERWISE MANDATED BY LAW, LICENSOR SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN ANY WAY CONNECTED WITH
(I) THE USE OF THE TIGRIS SOFTWARE OR ANY DELAY OR INABILITY TO USE THE TIGRIS SOFTWARE (OR ANY LINKED SITES), (II) THE ACCURACY, COMPLETENESS OR RELIABILITY OF ANY INFORMATION, SOFTWARE, PRODUCTS OBTAINED THROUGH THE TIGRIS SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE TIGRIS SOFTWARE OR THE INTERNET GENERALLY, OR (III) THIS AGREEMENT, WHETHER BASED ON CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. IF THE FOREGOING IS HELD INAPPLICABLE OR UNENFORCEABLE, THEN IN NO EVENT WILL LICENSOR BE LIABLE FOR DAMAGES ARISING OUT OF THE AGREEMENT IN AMOUNTS GREATER THAN THE TOTAL FEES PAID TO LICENSOR BY LICENSEE DURING THE QUARTER IN WHICH THE CAUSE OF ACTION AROSE. This clause shall not impair the U.S. Government’s right to recover for fraud or crimes arising out of or related to this Contract under any federal fraud statute, including the False Claims Act, 31 USC 3729-3733. Furthermore, this clause shall not impair nor prejudice the U.S Government’s right to express remedies provided in the GSA MAS Schedule contract (e.g., clause 552.238-75 – Price Reductions, clause 52.212-4(h) – Patent Indemnification, and GSAR 552.215-72 – Price Adjustment – Failure to Provide Accurate Information).

d. Any claim or action brought by LICENSEE pursuant to this Agreement (including the PO) must be brought within one year after the date the claim or action arises, whether or not the LICENSEE bringing the claim or action has actual knowledge of such claim or action.
54151S Labor Categories

TTK-01.2 Technical Writer

The Technical Writer helps TalaTek achieve the highest level of customer satisfaction by delivering consistently high-quality work products. Our team has customer satisfaction as a primary quality objective. TalaTek structures our service delivery around “what” service or quality level is required, as opposed to “how” the team should perform the work (i.e., results, not compliance). The objective of the Technical Writer is to ensure the “what” (work products) meet the customer’s expected outcomes or performance objectives.

The Technical Writer position requires the following abilities:

- Review and update the TalaTek Quality Assurance Surveillance Plan (QASP). The QASP defines work products to be reviewed and the scope and level of review required. The scope of the review may encompass entire documents or may require sampling. Depending on the level of effort, the QASP will specify that reviews check for quality, accuracy, completeness, and compliance with the TalaTek process, as well as compliance with applicable customer process and standards and NIST publication standards.
- Perform scheduled reviews of work products following the QASP. This will include reviewing documents and control analysis produced by TalaTek teams.
- Identify needed improvements in reviewed documents and/or associated process.
- Provide feedback and guidance to document authors/process owner based on above Quality Assurance (QA) review. Feedback will generally include comments in documents and checklists; it may also include tracking changes.
- Perform ad hoc or, as requested, reviews with feedback for quality, accuracy and completeness, documents and control analysis results.
- Review other TalaTek documents related to Business Development, FedRAMP, and other efforts, and provide feedback and guidance.
- Review the overall status of projects and progress to identify omissions and ensure TalaTek processes and customer regulations and policies are following the identified repeatable processes.
- Ensure that defined processes are consistently implemented across all teams/products and service delivery areas. Provide feedback for process improvement, training requirements, or resource allocation based on root cause analysis of identified risk area.
- Coordinate to ensure work products reflect proper grammar, spelling, punctuation, formats, etc.
- Develop metrics for quarterly quality report for presentation to TalaTek and client management.
- Manage day-to-day operational aspects of a documentation and deliverables.
- Prepare deliverables drafted by team before passing to client.
- Effectively applies technical standards to customer deliverables.
- Prepare for engagement reviews and QA procedures.
- Ensure deliverables are complete, current, and stored appropriately.
- Utilize previous experience in the IT risk and/or IT security field to ensure consistency across functional and technical groups.
- Identify, communicate, and manage all deliverable tasks.
- Must possess proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership.
- Education/Experience: Bachelor’s degree in a relevant field or equivalent is preferred and seven (7) years of IT experience.

The Technical Writer will:

- Build the annual QASP. The QASP will identify:
  - Work products to be reviewed,
• Schedule for review,
  • Type and level of review required, and
  • Standards against which the work products will be measured.

• Analyze work products according to the QASP.
• When reviewing the analysis of NIST controls, the Technical Writer will consider:
  • Is analysis complete and up to date?
  • Has the analysis addressed NIST and client requirements adequately?
  • Does the analysis support the conclusion?
  • Has evidence been supplied to support the conclusion?
  • Does the analysis comply with TalaTek procedures?

• When reviewing System Security Plans; Risk Assessments; client Risk Acceptances; Privacy Impact Assessment (PIA); Program Security Categorization; quarterly status reports to the AO, ISSO, and CISO, and an annual update to the AO; and other client-required documents, the Technical Writer will consider:
  • Project plans
  • TalaTek procedures
  • Client requirements, policies, procedures, standards, and processes
  • NIST publications

• Provide client support and attend meetings as needed.
• Advise project managers and TalaTek staff on needed changes to TalaTek policies and procedures based on the results of the QA process.
• Develop and implement new processes based on changes to the TalaTek QASP.

Expectations – The successful candidate will:

• Work independently with minimal supervision.
• Know how to seek out guidance/assistance from appropriate resources when necessary.
• Apply great attention to detail when reviewing work products, documents, and deliverables.
• Be capable of communicating complex issues efficiently, effectively, and diplomatically to peers, TalaTek leadership, and clients.
• Multitask effectively.
• Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Technical Writer will, at minimum, have:

• Bachelor’s degree in Computer Information Systems or equivalent is preferred and seven (7) years of experience in IT
• Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing Training requirements of the Technical Writer:

• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Pursue ongoing research and training associated with being informed and aware of current organizational QA best practices.
• Utilize training and information resources, which include:
  • The American Society for Quality (http://asq.org/knowledge-center/index.html)
  • National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
Products: SIN 518210C TiGRIS SaaS HACS SIN 54151HACS SIN 54151S SIN OLM

- Information Systems Audit and Control Association ([https://www.isaca.org/Pages/default.aspx](https://www.isaca.org/Pages/default.aspx))
- American Association for Laboratory Accreditation ([https://www.a2la.org/index.cfm](https://www.a2la.org/index.cfm))
TTK-02.2 Project Manager

The TalaTek Project Manager role requires a project management professional with a proven approach for rapidly moving organizations to a culture of disciplined planning and execution of strategic projects and programs. The TalaTek Project Manager possesses past experience in a range of practical environments with a proven record of services and delivery of IT project management. The Project Manager’s role is to stay on top of all aspects of the TalaTek project: process, interpersonal, and organizational and to forge a spirit of cooperation and achievement among the diverse team members. The Project Manager is expected to deal effectively with all the contingencies, foreseen and unforeseen, ensuring delivery on budget and according to timeline set by customer.

The Project Manager will:

- Create and execute project work plans and revise as appropriate to meet changing client needs and requirements.
- Manage day-to-day operational aspects of a project and scope.
- Review deliverables prepared by team before passing to client.
- Effectively apply our methodology and enforce project standards.
- Prepare for engagement reviews and QA procedures.
- Minimize TalaTek and TalaTek client exposure and risk on projects.
- Ensure project documents are complete, current, and stored appropriately.
- Utilize previous experience working in IT risk and/or IT security to ensure consistency across functional and technical groups.
- Build and maintain a good working relationship with the client and team members.
- Effectively communicate to TalaTek leadership, project teams, clients, and supporting organizations to ensure expectations are known and consistently managed.
- Identify, communicate, and manage all project risks.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing work products, documents, and deliverables.
- Be capable of communicating complex issues efficiently, effectively, and diplomatically to peers, TalaTek leadership, and clients.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Project Manager will, at minimum, have:

- Project Management Professional (PMP) certification (recommended)
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership
- Proficiency in Microsoft Project
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and four (4) years of experience in IT Project Management

Ongoing Training requirements of the Project Manager:

- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Pursue ongoing research and training associated with being informed and aware of up-to-date project management best practices.
Utilize training and information resources, which include:

- Project Management Institute (http://www.pmi.org/en.aspx)
- National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- American Association for Laboratory Accreditation (https://www.a2la.org/index.cfm)
TTK-02.3 Program Manager

The TalaTek Program Manager role requires a project management professional with a proven approach for rapidly moving organizations to a culture of disciplined planning and execution of multiple strategic projects and programs. The TalaTek Program Manager possesses past experience in a range of practical environments with a proven record of services and delivery of multiple concurrent project management contracts. The Program Manager's role is to stay on top of all aspects of TalaTek projects: process, interpersonal, and organizational and to forge a spirit of cooperation and achievement among the diverse teams and team members. The Program Manager is expected to deal effectively with all the contingencies, foreseen and unforeseen, ensuring delivery on budget and according to timeline set by customer for all projects.

The Program Manager will:

- Create and execute project work plans and revise as appropriate to meet changing client needs and requirements.
- Manage day-to-day operational aspects of multiple projects and scopes.
- Review deliverables prepared by teams before passing to client.
- Effectively apply our methodology and enforce program and project standards.
- Prepare for engagement reviews and QA procedures.
- Minimize TalaTek and TalaTek client exposure and risk across projects.
- Ensure project documents are complete, current, and stored appropriately.
- Utilize previous experience working in IT risk and/or to ensure consistency across functional and technical groups.
- Build and maintain a good working relationship with clients and teams.
- Effectively communicate to TalaTek leadership, project teams, clients, and supporting organizations to ensure expectations are known and consistently managed.
- Identify, communicate, and manage all projects' risks.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing work products, documents, and deliverables.
- Be capable of communicating complex issues efficiently, effectively, and diplomatically to peers, TalaTek leadership, and clients.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Program Manager will, at minimum, have:

- Project Management Professional (PMP) certification (recommended)
- Proficient written and verbal communication skills in order to effectively interact with clients, project teams, and TalaTek leadership
- Proficiency in Microsoft Project
- Bachelor's degree in Computer Information Systems or equivalent is preferred and eight (8) years of experience in IT and/or Program Management

Ongoing Training requirements of the Program Manager:

- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Pursue ongoing research and training associated with being informed and aware of up-to-date project management best practices.
• Utilize training and information resources, which include:
  o Project Management Institute (http://www.pmi.org/en.aspx)
  o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  o American Association for Laboratory Accreditation (https://www.a2la.org/index.cfm)
TTK-03.2 Deputy Quality System Manager

The **Deputy Quality System Manager** possesses past experience ensuring the maintenance of Quality Systems. The Deputy Quality System Manager must be able to communicate effectively with the Quality System Manager on all matters related to the performance of the Quality System and report areas needing improvement. Additionally, the Deputy Quality System Manager is expected to deal effectively with all contingencies and assist the Quality System Manager with the delivery of a Quality System as outlined in the Quality System Manual. In the absence of the Quality System Manager, the Deputy Quality System Manager shall ensure the maintenance of a Quality System in accordance with ISO/IEC 17020:2012, *Conformity assessment—Requirements for the operation of various types of bodies performing inspection.*

The **Deputy Quality System Manager** will:

- Assist with ensuring that all processes needed for the Quality System are established, implemented, and maintained.
- Report to the Quality System Manager on the performance of the Quality System and any changes needed for improvement.
- Assist the Quality System Manager in communicating with external assessment bodies on all matters related to the external accreditation process.
- Ensure that a document control procedure is adopted to approve, review, and update all changes to critical documents within the scope of the Quality System.
- Establish and maintain records to be provided as evidence that the Quality System is being followed and that there is a system in place for the identification, storage, protection, retrieval, retention time, and disposal of such records.
- Track the review of the Quality System and ensure that the review is conducted on planned intervals to ensure its continuing suitability, adequacy, and effectiveness. This review includes assessing opportunities for improvement and the need for changes to the Quality System.
- Induct all new TalaTek team members into the requirements of the Quality System related to their roles and responsibilities. Provide update trainings as necessary.
- Ensure that all suppliers used by TalaTek are selected and evaluated/re-evaluated and that records of this assessment are maintained.
- Conduct internal audits of the Quality System in accordance with ISO 17020:2012, verifying that the Quality System conforms to planned internal audit arrangements and is effectively implemented and maintained, and taking appropriate action to identify when this is not the case.
- Contribute to continual improvements to the Quality System, ensuring that evidence of corrective and preventative actions taken are recorded and reviewed.

**Expectations** – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

**Requirements** – **Deputy Quality System Manager** will, at a minimum, have:

- Training on ISO 17020:2012, Conformity assessment – Requirements for the operation of various types of bodies performing inspection. (recommended)
• Proficient written and verbal communication skills in order to effectively interact with clients, project team, Quality System Manager, and TalaTek leadership
• Bachelor’s degree in Computer Information Systems or equivalent is preferred and four (4) years of experience in IT

Ongoing Training requirements of the **Deputy Quality System Manager**:

• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Pursue ongoing research and training associated with being informed and aware of current organizational quality assurance best practices.
• Utilize training and information resources, which include:
  o National Institute of Standards and Technology ([http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html))
  o Information Systems Audit and Control Association ([https://www.isaca.org/Pages/default.aspx](https://www.isaca.org/Pages/default.aspx))
  o American Association for Laboratory Accreditation ([https://www.a2la.org/index.cfm](https://www.a2la.org/index.cfm))
TTK-03.3 Quality System Manager

The TalaTek Quality System Manager possesses past experience ensuring the development and maintenance of Quality Systems. The Quality System Manager must be able to communicate effectively on all matters related to the performance of the Quality System and report areas needing improvement. Additionally, the Quality System Manager is expected to deal effectively with all contingencies (both internal and external), foreseen and unforeseen, and ensuring delivery of a Quality System as outlined in the Quality System Manual. The Quality System Manager shall ensure the maintenance of a Quality System in accordance with ISO/IEC 17020:2012, Conformity assessment—Requirements for the operation of various types of bodies performing inspection.

The Quality System Manager will:

- Ensure that processes needed for the Quality System are established, implemented, and maintained.
- Report to top management on the performance of the Quality System and any changes needed for improvement.
- Ensure the promotion of customer requirements throughout TalaTek.
- Liaise with external assessment bodies on all matters related to the external accreditation process.
- Ensure that a document control procedure is adopted and followed to approve, review, and update all changes to critical documents within the scope of the Quality System.
- Establish and maintain records to be provided as evidence that the Quality System is being followed and that there is a system in place for the identification, storage, protection, retrieval, retention time, and disposal of such records.
- Track the review of the Quality System and ensure that the review is conducted on planned intervals to ensure its continuing suitability, adequacy, and effectiveness. This review includes assessing opportunities for improvement and the need for changes to the Quality System.
- Ensure that Quality System Objectives are set by TalaTek senior management for measuring the performance of the Quality System and that these measures are regularly reviewed.
- Induct all new TalaTek team members into the requirements of the Quality System related to their roles and responsibilities. Provide update trainings as necessary.
- Ensure that all suppliers used by TalaTek are selected and evaluated/re-evaluated and that records of this assessment are maintained.
- Manage the implementation and maintenance of the TalaTek ISO 17020:2012 internal audit program, verifying that the Quality System conforms to planned internal audit arrangements and is effectively implemented and maintained, and taking appropriate action to identify when this is not the case.
- Analyze data relating to the effectiveness of the Quality System and evaluate on a continuous basis where improvements to the Quality System can be made based on the findings from the analysis. This can also include data generated as a result of monitoring and measurement from other relevant external sources.
- Coordinate continual improvements to the Quality System, ensuring that evidence of corrective and preventative actions taken are recorded and reviewed.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.
Requirements – The **Quality System Manager** will, at a minimum, have:

- Training on ISO 17020:2012, Conformity assessment – Requirements for the operation of various types of bodies performing inspection. (recommended)
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and seven (7) years of experience in IT

Ongoing Training requirements of the **Quality System Manager**:

- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Pursue ongoing research and training associated with being informed and aware of current organizational quality assurance best practices.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology ([http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html))
  - Information Systems Audit and Control Association ([https://www.isaca.org/Pages/default.aspx](https://www.isaca.org/Pages/default.aspx))
  - American Association for Laboratory Accreditation ([https://www.a2la.org/index.cfm](https://www.a2la.org/index.cfm))
TTK-04.3 Senior Information Security Consultant

The Senior Information Security Consultant possesses past experience in a range of practical environments with a proven record of services and delivery of IT project management. The Senior Information Security Consultant will ensure effective delivery of the overall Security Assessment process according to NIST SP 800-37. Additionally, the Senior Information Security Consultant is expected to deal effectively as a Project Manager role with all contingencies, foreseen and unforeseen, and ensuring delivery on or under budget and according to the timeline set by the customer.

The Senior Information Security Consultant will:

- Manage all SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop and complete risk assessments based on NIST standards to ensure the Information Assurance (IA) design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology; supervise other team members to complete project requirements effectively.
- Identify, document, and report security issues and concerns to officials; follow up on action items to resolve security issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Perform the technical security architect role, creating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Required to carry out all inspections in accordance with ISO/IEC 17020:2012, Conformity assessment – Requirements for the operation of various types of bodies performing inspection.
- Support and provide in-depth understanding of the TalaTek process and the ability to implement action items, manage reports, and provide overall systems support.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Capable of communicating complex issues efficiently and effectively to TalaTek team and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Expectations – a successful candidate will:

- Work independently to optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, and key management tools, etc.).
- Lead the team in conducting security risk assessments, vector attack, and penetration testing, and vulnerability assessments of networks and resources attached to the network.
- Identify, document, and report security issues and concerns to officials, and follow up on action items to resolve security issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Perform the technical security architect role, creating design documents and instructional materials for non-security focused teams, detail technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption and key management tools, etc.).
Requirements – The Senior Information Security Consultant will, at minimum, have:

- CISSP certification, or can attain within six (6) months of hire
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and six (6) years of experience in Information Security
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing training requirements of the Senior Information Security Consultant:

- Progressively pursue EC-Council certifications, such as Certified Ethical Hacker (CEH), Licensed Penetration Tester, etc. – order of certifications obtained should be determined based on an ongoing evaluation of candidate’s skills assessments.
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and the tools associated with completing security assessments – completing vendor-specific training as necessary, such as Qualys, Nessus, etc.
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloud.cio.gov/fedramp)
  - Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  - International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  - Project Management Institute (http://www.pmi.org/en.aspx)
  - Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-05.1 Junior Continuous Monitoring Analyst

The **Junior Continuous Monitoring Analyst** is an entry-level position requiring the following abilities:

- Support SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
- Identify, document, and report security issues and concerns to TalaTek leadership and officials.
- Follow up on action items to resolve IT and program security issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support the technical security architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

The **Junior Continuous Monitoring Analyst** will:

- Support the development of annual Continuous Monitoring Plans.
- Analyze controls each quarter according to plan, following TalaTek processes and workflows as required, in a timely manner. Controls analysis will be phased through the quarter. Analyzing status includes:
  - Is analysis complete and accurate?
  - Does ISO or ISSO have additional requirements?
  - Are there new NIST or industry requirements?
  - Request new or renewed evidence or confirmation of practice for current continuous monitoring period.
  - Analyze new information provided; responding to evidence provided by the client within three (3) working days.
  - Document decisions regarding implementation/compliance status.
  - Update centralized repository to reflect compliance status and attaching evidence supporting decisions.
  - Read and answer all work e-mails within one (1) working day.
  - Support preparation of client-required documentation:
  - Meeting status agenda and minutes
  - Controls and POA&Ms under review report
  - Attend client status meetings and TalaTek status meetings
  - Update central repository with results of the meetings within two (2) working days after the working meeting
  - Update System Security Plan (SSP) and updated Risk Assessment (RA) on schedule
  - Review/revision of the Privacy Impact Assessment (PIA)
  - Review/revision of the Program Security Categorization
  - Provide an updated POA&M report as needed
  - TalaTek monthly status reports
  - Quarterly status reports to the AO, ISSO, and CISO, and an annual update to the AO
  - Annual review and renewals of Risk Acceptances for risk-based decisions
Authorized Multiple Award Schedule Catalog/Price List
Contract Number: GS-35F-399DA

- Annual year-end review
- Other client-required documents

- Provide onsite (client) support and attend meetings as needed.
- Respond to audit requests and findings.
  - Supply documents requested by auditor

- Conduct onsite visits to client site(s) for:
  - Security control and documentation review
  - Site inspections

- Create White Papers on security topics as needed for TalaTek/client.
- Support internal QA efforts on an ongoing basis.
- Develop and implement new processes based on changes to TalaTek, client and/or NIST requirements.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Junior Continuous Monitoring will, at minimum, have:

- CompTIA Security+ certification within one (1) to two (2) years of beginning employment at TalaTek (recommended)
- Aptitude for processing complex IT concepts
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and two (2) years of experience in Information Security

Ongoing Training requirements of the Junior Continuous Monitoring Analyst:

- Progressively pursue (ISC)² and ISACA certifications, such as Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA), etc. – order of certifications obtained should be determined based on ongoing evaluation of candidate’s skills assessments.
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results of ongoing observations and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
Products:

- SIN 518210C TiGRIS SaaS HACS
- SIN 54151HACS
- SIN 54151S
- SIN OLM

- FedRAMP (http://cloud.cio.gov/fedramp)
- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
- Project Management Institute (http://www.pmi.org/en.aspx)
- Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-05.2 Continuous Monitoring Analyst

Information Security Continuous Monitoring (ISCM) is a team effort. The team consists of a Project Manager, Security Control Analysts, and Quality Control personnel. Analysts are responsible for ongoing monitoring of specific families of controls. Analysts monitor the control families to reflect the current status of controls in near real-time. The Continuous Monitoring Analyst is a mid-level position requiring the following abilities:

- Manage a team, as described above, to achieve client/task goals, deadlines, and risk management objectives, and report to senior management on issues and progress, as well as make recommendations for process improvement.
- Be part of the ISCM team, involved in all tasks, and with experience providing: project planning, guidance, mentoring, and support to the various roles within the team, such as Project Manager QA and Security Analysts.

The Continuous Monitoring Analyst will:

- Develop and support the implementation of the annual ISCM Plan.
- Supervise and provide subject matter expertise for control analysis each quarter according to the ISCM Plan, following TalaTek processes in a timely manner. Control analysis will be phased throughout the quarter, with initial analysis of all controls completed within 45 days after the quarter starts.
- Provide QA for control analysis accuracy and level of detail in context of the system’s risk and categorization:
  - Was previous analysis complete and accurate?
  - Does ISO/IO or ISSO have additional requirements?
  - Are there new organizational or NIST requirements?
  - Are there related controls or POA&M items that need to be addressed?
  - Understand the concept of inherited controls, common control providers, and assess risks accordingly.
- Ensure collection of new or renewed evidence and confirm that supporting evidence for control analysis is accurate and meets security standards.
- Analyze new information provided and respond to evidence collected within three (3) working days.
- Responsible for final document decisions regarding implementation/compliance status.
- Make sure controls status is up to date and reflects compliance status, and attach evidence supporting the decision.
- Read and answer emails within one (1) working day.
- Support preparation of client-required documents:
  - Bi-weekly status agenda and minutes
  - Bi-weekly controls and POA&Ms under review report
  - Attend client bi-weekly status meetings and TalaTek weekly status meetings
  - Update related systems with results of the meetings within two (2) working days after the TalaTek working meeting (this includes entering comments, updating status, attaching documents)
  - Update the System Security Plan (SSP) and Risk Assessment (RA)
  - Review/revision of the Privacy Impact Assessment (PIA) and PTA, if needed
  - Review/revision of the Program Security Categorization consistent with FIPS 199
  - Provide an updated POA&M report each quarter with up-to-date Recommended Actions for each outstanding POA&M
  - Monthly status reports
  - Quarterly status reports to the AO, ISSO, and CISO, and annual update to the AO
  - Annual review and renewals of Risk Acceptances
  - Annual year-end review
Products:

- SIN 518210C TiGRIS SaaS HACS
- SIN 54151HACS SIN 54151S
- SIN OLM

Other required documents (i.e., Classification and Determination memo, PIA Executive Summary, Bi-annual Cycle memo, etc.)

- At a minimum, provide onsite (client) support one (1) day per week for meetings as needed.
- Read and answer emails from client quickly on the same day, if possible.
- Respond to audit requests and findings.
- Supply documents requested by auditor.
- Prepare Request for Closure of Findings (RCFs) and related documents.
- Conduct onsite visits to client sites, if needed, for:
  - Document review
  - Site inspections
- Create White Papers on security topics as needed.
- Perform internal QA.
- Develop and implement new processes based on changes to client and/or NIST requirements.
- Support TalaTek new business research and proposals, as needed.
- Respond to other requests as needed.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients. Immediately acknowledge that requests were received, provide a quick response to requests, and deliver a very professional level of product.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Continuous Monitoring Analyst will, at minimum, have:

- Bachelor's degree in Computer Information Systems or equivalent is preferred and four (4) years of IT experience in Information Systems
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing Training requirements of the Continuous Monitoring Analyst/Team Lead:

- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results on ongoing observation and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloudcio.gov/fedramp)
- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
- Project Management Institute (http://www.pmi.org/en.aspx)
- Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-05.3 Senior Continuous Monitoring Analyst

The Senior Continuous Monitoring Analyst is a senior-level position requiring the following abilities:

- Manage SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
- Identify, document, and report security issues and concerns to officials.
- Follow up on action items to resolve IT and program security issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support the technical security architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

The Senior Continuous Monitoring Analyst will:

- Build annual Continuous Monitoring Plans.
- Analyze controls each quarter according to plan, following TalaTek processes and workflows, as required, in a timely manner. Controls analysis will be phased through the quarter. Analyzing status includes:
  - Is analysis complete and accurate?
  - Does ISO or ISSO have additional requirements?
  - Are there new NIST or industry requirements?
- Request new or renewed evidence or confirmation of practice for current continuous monitoring period.
- Analyze new information provided; respond to evidence provided by the client within three (3) working days.
- Document decisions regarding implementation/compliance status.
- Update centralized repository to reflect compliance status and attaching evidence supporting decisions.
- Read and answer all work e-mails within one (1) working day.
- Support preparation of client-required documentation:
  - Meeting status agenda and minutes
  - Controls and POA&Ms under review report
  - Attend client status meetings and TalaTek status meetings
  - Update central repository with results of the meetings within two (2) working days after the working meeting
  - Updated System Security Plan (SSP) and updated Risk Assessment (RA) on schedule
  - Review/revision of the Privacy Impact Assessment (PIA)
  - Review/revision of the Program Security Categorization
  - Provide an updated POA&M report as needed
  - TalaTek monthly status reports
Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Senior Continuous Monitoring will, at minimum, have:

- CISSP certification and continuing related professional development, or can attain within six (6) months of hire (recommended)
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and eight (8) years of IT experience in Information Systems
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing Training requirements of the Senior Continuous Monitoring Analyst:

- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results on ongoing observation and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloud.cio.gov/fedramp)
- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
- Project Management Institute (http://www.pmi.org/en.aspx)
- Cloud Security Alliance (https://cloudsecurityalliance.org/)
518210C – Labor Categories

TTK-11.2 Cloud Services Technical Writer

The Cloud Services Technical Writer helps TalaTek achieve the highest level of customer satisfaction by delivering consistently high-quality cloud services work products. Our team has customer satisfaction as a primary quality objective. TalaTek structures our service delivery around “what” service or quality level is required, as opposed to “how” the team should perform the work (i.e., results, not compliance). The objective of the Cloud Services Technical Writer is to ensure the “what” (work products) meet the customer’s expected outcomes or performance objectives.

The Cloud Services Technical Writer position requires the following abilities:

- Review and update the TalaTek Quality Assurance Surveillance Plan (QASP). The QASP defines work products to be reviewed and the scope and level of review required. The scope of the review may encompass entire documents or may require sampling. Depending on the level of effort, the QASP will specify that reviews check for quality, accuracy, completeness, and compliance with the TalaTek process, as well as compliance with applicable customer process and standards and NIST publication standards.
- Perform scheduled reviews of cloud work products following the QASP. This will include reviewing cloud documents and control analysis produced by TalaTek teams.
- Identify needed improvements in reviewed cloud documents and/or associated process.
- Provide feedback and guidance to document authors/process owner based on above Quality Assurance (QA) review. Feedback will generally include comments in documents and checklists; it may also include tracking changes.
- Perform ad hoc or, as requested, reviews with feedback for quality, accuracy and completeness, documents and control analysis results.
- Review other TalaTek documents related to Business Development, FedRAMP, and other efforts, and provide feedback and guidance.
- Review the overall status of projects and progress to identify omissions and ensure TalaTek processes and customer regulations and policies are following the identified repeatable processes.
- Ensure that defined processes are consistently implemented across all teams/products and service delivery areas. Provide feedback for process improvement, training requirements, or resource allocation based on root cause analysis of identified risk area.
- Coordinate to ensure cloud work products reflect proper grammar, spelling, punctuation, formats, etc.
- Develop metrics for quarterly quality report for presentation to TalaTek and client management.
- Manage day-to-day operational aspects of a documentation and deliverables.
- Prepare deliverables drafted by team before passing to client.
- Effectively applies technical standards to customer deliverables.
- Prepare for engagement reviews and QA procedures.
- Ensure deliverables are complete, current, and stored appropriately.
- Utilize previous experience in the IT risk and/or IT security field to ensure consistency across functional and technical groups.
- Identify, communicate, and manage all deliverable tasks.
- Must possess proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership.
- Education/Experience: Bachelor’s degree in a relevant field or equivalent is preferred and seven (7) years of IT and/or cloud services experience.

The Cloud Services Technical Writer will:

- Build the annual QASP. The QASP will identify:
  - Work products to be reviewed,
• Schedule for review,
  • Type and level of review required, and
  • Standards against which the work products will be measured.

• Analyze work products according to the QASP.
• When reviewing the analysis of NIST controls, the Cloud Services Technical Writer will consider:
  • Is analysis complete and up to date?
  • Has the analysis addressed NIST and client requirements adequately?
  • Does the analysis support the conclusion?
  • Has evidence been supplied to support the conclusion?
  • Does the analysis comply with TalaTek procedures?

• When reviewing System Security Plans; Risk Assessments; client Risk Acceptances; Privacy Impact Assessment (PIA); Program Security Categorization; quarterly status reports to the AO, ISSO, and CISO, and an annual update to the AO; and other client-required documents, the Cloud Services Technical Writer will consider:
  • Project plans
  • TalaTek procedures
  • Client requirements, policies, procedures, standards, and processes
  • NIST publications

• Provide client support and attend meetings as needed.
• Advise project managers and TalaTek staff on needed changes to TalaTek policies and procedures based on the results of the QA process.
• Develop and implement new processes based on changes to the TalaTek QASP.

**Expectations** – The successful candidate will:

• Work independently with minimal supervision.
• Know how to seek out guidance/assistance from appropriate resources when necessary.
• Apply great attention to detail when reviewing work products, documents, and deliverables.
• Be capable of communicating complex issues efficiently, effectively, and diplomatically to peers, TalaTek leadership, and clients.
• Multitask effectively.
• Capitalize on strengths and identify areas of opportunities for improvement.

**Requirements** – The **Cloud Services Technical Writer** will, at minimum, have:

• Bachelor’s degree in Computer Information Systems or equivalent is preferred and seven (7) years of experience in IT and/or cloud services
• Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

**Ongoing Training requirements of the Cloud Services Technical Writer:**

• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Pursue ongoing research and training associated with being informed and aware of current organizational QA best practices.
• Utilize training and information resources, which include:
  • The American Society for Quality ([http://asq.org/knowledge-center/index.html](http://asq.org/knowledge-center/index.html))
  • National Institute of Standards and Technology ([http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html))
o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
o American Association for Laboratory Accreditation (https://www.a2la.org/index.cfm)
TTK-12.2 Cloud Services Project Manager

The TalaTek Cloud Services Project Manager role requires a project management professional with a proven approach for rapidly moving organizations to a culture of disciplined planning and execution of strategic cloud services projects and programs. The TalaTek Cloud Services Project Manager possesses past experience in a range of practical environments with a proven record of services and delivery of cloud services project management. The Cloud Services Project Manager's role is to stay on top of all aspects of the TalaTek cloud services project: process, interpersonal, and organizational and to forge a spirit of cooperation and achievement among the diverse team members. The Cloud Services Project Manager is expected to deal effectively with all the contingencies, foreseen and unforeseen, ensuring delivery on budget and according to timeline set by customer.

The Cloud Services Project Manager will:

- Create and execute cloud services project work plans and revise as appropriate to meet changing client needs and requirements.
- Manage day-to-day operational aspects of a cloud services project and scope.
- Review deliverables prepared by team before passing to client.
- Effectively apply our methodology and enforce project standards.
- Prepare for engagement reviews and QA procedures.
- Minimize TalaTek and TalaTek client exposure and risk on cloud services projects.
- Ensure project documents are complete, current, and stored appropriately.
- Utilize previous experience working in IT risk and/or cloud services to ensure consistency across functional and technical groups.
- Build and maintain a good working relationship with the client and team members.
- Effectively communicate to TalaTek leadership, project teams, clients, and supporting organizations to ensure expectations are known and consistently managed.
- Identify, communicate, and manage all project risks.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing work products, documents, and deliverables.
- Be capable of communicating complex issues efficiently, effectively, and diplomatically to peers, TalaTek leadership, and clients.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Cloud Services Project Manager will, at minimum, have:

- Project Management Professional (PMP) certification (recommended)
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership
- Proficiency in Microsoft Project
- Bachelor's degree in Computer Information Systems or equivalent is preferred and four (4) years of experience in IT and/or cloud services Project Management

Ongoing Training requirements of the Cloud Services Project Manager:

- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
Pursue ongoing research and training associated with being informed and aware of up-to-date project management best practices.

Utilize training and information resources, which include:

- Project Management Institute (http://www.pmi.org/en.aspx)
- National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- American Association for Laboratory Accreditation (https://www.a2la.org/index.cfm)
TTK-13.1 Junior Cloud Continuous Monitoring Analyst

The **Junior Cloud Continuous Monitoring Analyst** is an entry-level position requiring the following abilities:

- Support SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop cloud risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
- Identify, document, and report cloud issues and concerns to TalaTek leadership and officials.
- Follow up on action items to resolve IT and program cloud issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support the technical cloud architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for cloud incident monitoring, audit and logging procedures for enhancing the client’s cloud infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

The **Junior Cloud Continuous Monitoring Analyst** will:

- Support the development of annual Continuous Monitoring Plans.
- Analyze controls each quarter according to plan, following TalaTek processes and workflows as required, in a timely manner. Controls analysis will be phased through the quarter. Analyzing status includes:
  - Is analysis complete and accurate?
  - Does ISO or ISSO have additional requirements?
  - Are there new NIST or industry requirements?
  - Request new or renewed evidence or confirmation of practice for current continuous monitoring period.
  - Analyze new information provided; responding to evidence provided by the client within three (3) working days.
  - Document decisions regarding implementation/compliance status.
  - Update centralized repository to reflect compliance status and attaching evidence supporting decisions.
  - Read and answer all work e-mails within one (1) working day.
  - Support preparation of client-required documentation:
    - Meeting status agenda and minutes
    - Controls and POA&Ms under review report
    - Attend client status meetings and TalaTek status meetings
    - Update central repository with results of the meetings within two (2) working days after the working meeting
    - Update System Security Plan (SSP) and updated Risk Assessment (RA) on schedule
    - Review/revision of the Privacy Impact Assessment (PIA)
    - Review/revision of the Program Security Categorization
    - Provide an updated POA&M report as needed
    - TalaTek monthly status reports
    - Quarterly status reports to the AO, ISSO, and CISO, and an annual update to the AO
Authorized Multiple Award Schedule Catalog/Price List
Contract Number: GS-35F-399DA

- Annual review and renewals of Risk Acceptances for risk-based decisions
- Annual year-end review
- Other client-required documents
- Provide onsite (client) support and attend meetings as needed.
- Respond to audit requests and findings.
  - Supply documents requested by auditor
- Conduct onsite visits to client site(s) for:
  - Security control and documentation review
  - Site inspections
- Create White Papers on security topics as needed for TalaTek/client.
- Support internal QA efforts on an ongoing basis.
- Develop and implement new processes based on changes to TalaTek, client and/or NIST requirements.

Expectations – The successful candidate will:
- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Junior Cloud Continuous Monitoring will, at minimum, have:
- CompTIA Security+ certification within one (1) to two (2) years of beginning employment at TalaTek (recommended)
- Aptitude for processing complex IT and/or cloud concepts
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and two (2) years of experience in Information Security and/or cloud security

Ongoing Training requirements of the Junior Cloud Continuous Monitoring Analyst:
- Progressively pursue (ISC)² and ISACA certifications, such as Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA), etc. – order of certifications obtained should be determined based on ongoing evaluation of candidate’s skills assessments.
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results of ongoing observations and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
- Utilize training and information resources, which include:
o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html) 
o FedRAMP (http://cloud.cio.gov/fedramp) 
 o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx) 
 o International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/) 
 o Project Management Institute (http://www.pmi.org/en.aspx) 
 o Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-13.2 Cloud Continuous Monitoring Analyst

Information Security Continuous Monitoring (ISCM) is a team effort. The team consists of a Cloud Project Manager, Cloud Control Analysts, and Cloud Quality Control personnel. Cloud Analysts are responsible for ongoing monitoring of specific families of controls. Cloud Analysts monitor the control families to reflect the current status of controls in near real-time. The **Cloud Continuous Monitoring Analyst** is a mid-level position requiring the following abilities:

- Manage a team, as described above, to achieve client/task goals, deadlines, and risk management objectives, and report to senior management on cloud issues and progress, as well as make recommendations for process improvement.
- Be part of the ISCM team, involved in all tasks, and with experience providing: project planning, guidance, mentoring, and support to the various roles within the team, such as Project Manager QA and Cloud Analysts.

The **Cloud Continuous Monitoring Analyst** will:

- Develop and support the implementation of the annual ISCM Plan.
- Supervise and provide subject matter expertise for control analysis each quarter according to the ISCM Plan, following TalaTek processes in a timely manner. Control analysis will be phased throughout the quarter, with initial analysis of all controls completed within 45 days after the quarter starts.
- Provide QA for control analysis accuracy and level of detail in context of the system’s risk and categorization:
  o Was previous analysis complete and accurate?
  o Does ISO/IO or ISSO have additional requirements?
  o Are there new organizational or NIST requirements?
  o Are there related controls or POA&M items that need to be addressed?
  o Understand the concept of inherited controls, common control providers, and assess risks accordingly.
- Ensure collection of new or renewed evidence and confirm that supporting evidence for control analysis is accurate and meets security standards.
- Analyze new information provided and respond to evidence collected within three (3) working days.
- Responsible for final document decisions regarding implementation/compliance status.
- Make sure cloud controls status is up to date and reflects compliance status, and attach evidence supporting the decision.
- Read and answer emails within one (1) working day.
- Support preparation of client-required documents:
  o Bi-weekly status agenda and minutes
  o Bi-weekly controls and POA&Ms under review report
  o Attend client bi-weekly status meetings and TalaTek weekly status meetings
  o Update related systems with results of the meetings within two (2) working days after the TalaTek working meeting (this includes entering comments, updating status, attaching documents)
  o Update the System Security Plan (SSP) and Risk Assessment (RA)
  o Review/revision of the Privacy Impact Assessment (PIA) and PTA, if needed
  o Review/revision of the Program Security Categorization consistent with FIPS 199
  o Provide an updated POA&M report each quarter with up-to-date Recommended Actions for each outstanding POA&M
  o Monthly status reports
  o Quarterly status reports to the AO, ISSO, and CISO, and annual update to the AO
  o Annual review and renewals of Risk Acceptances
  o Annual year-end review
Authorized Multiple Award Schedule Catalog/Price List
Contract Number: GS-35F-399DA

- Other required documents (i.e., Classification and Determination memo, PIA Executive Summary, Bi-annual Cycle memo, etc.)
- At a minimum, provide onsite (client) support one (1) day per week for meetings as needed.
- Read and answer emails from client quickly on the same day, if possible.
- Respond to audit requests and findings.
- Supply documents requested by auditor.
- Prepare Request for Closure of Findings (RCFs) and related documents.
- Conduct onsite visits to client sites, if needed, for:
  - Document review
  - Site inspections
- Create White Papers on security topics as needed.
- Perform internal QA.
- Develop and implement new processes based on changes to client and/or NIST requirements.
- Support TalaTek new business research and proposals, as needed.
- Respond to other requests as needed.

Expectations – The successful candidate will:
- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients. Immediately acknowledge that requests were received, provide a quick response to requests, and deliver a very professional level of product.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Cloud Continuous Monitoring Analyst will, at minimum, have:
- Bachelor's degree in Computer Information Systems or equivalent is preferred and four (4) years of IT experience in Information Systems and/or cloud security
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing Training requirements of the Cloud Continuous Monitoring Analyst:
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results on ongoing observation and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloud.cio.gov/fedramp)
Products: SIN 518210C TiGRIS SaaS HACS SIN 54151HACS SIN 54151S SIN OLM

- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
- Project Management Institute (http://www.pmi.org/en.aspx)
- Cloud Security Alliance (https://cloudsecurityalliance.org/)
**TTK-13.3 Senior Cloud Continuous Monitoring Analyst**

The **Senior Cloud Continuous Monitoring Analyst** is a senior-level position requiring the following abilities:

- Manage SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop cloud risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
- Identify, document, and report cloud issues and concerns to officials.
- Follow up on action items to resolve IT and program cloud issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support the technical cloud architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s cloud infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

The **Senior Cloud Continuous Monitoring Analyst** will:

- Build annual Continuous Monitoring Plans.
- Analyze controls each quarter according to plan, following TalaTek processes and workflows, as required, in a timely manner. Controls analysis will be phased through the quarter. Analyzing status includes:
  - Is analysis complete and accurate?
  - Does ISO or ISSO have additional requirements?
  - Are there new NIST or industry requirements?
- Request new or renewed evidence or confirmation of practice for current continuous monitoring period.
- Analyze new information provided; respond to evidence provided by the client within three (3) working days.
- Document decisions regarding implementation/compliance status.
- Update centralized repository to reflect compliance status and attaching evidence supporting decisions.
- Read and answer all work e-mails within one (1) working day.
- Support preparation of client-required documentation:
  - Meeting status agenda and minutes
  - Controls and POA&Ms under review report
  - Attend client status meetings and TalaTek status meetings
  - Update central repository with results of the meetings within two (2) working days after the working meeting
  - Updated System Security Plan (SSP) and updated Risk Assessment (RA) on schedule
  - Review/revision of the Privacy Impact Assessment (PIA)
  - Review/revision of the Program Security Categorization
  - Provide an updated POA&M report as needed
Products:

- SIN 518210C TiGRIS SaaS HACS
- SIN 54151HACS SIN 54151S
- SIN OLM

- TalaTek monthly status reports
- Quarterly status reports to the AO, ISSO, and CISO, and an annual update to the AO
- Annual review and renewals of Risk Acceptances for risk-based decisions
- Annual year-end review
- Other client-required documents

- Provide onsite (client) support and attend meetings as needed.
- Respond to audit requests and findings.
- Supply documents requested by auditor

- Conduct onsite visits to client site(s) for:
  - Security control and documentation review
  - Site inspections

- Create White Papers on security topics as needed for TalaTek/client.
- Perform internal QA on an ongoing basis.
- Develop and implement new processes based on changes to TalaTek, client, and/or NIST requirements.

**Expectations** – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

**Requirements** – The Senior Cloud Continuous Monitoring will, at minimum, have:

- CISSP certification and continuing related professional development, or can attain within six (6) months of hire (recommended)
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and eight (8) years of IT experience in Information Systems and/or cloud security
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing Training requirements of the Senior Cloud Continuous Monitoring Analyst:

- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results on ongoing observation and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloud.cio.gov/fedramp)
- Information Systems Audit and Control Association ([https://www.isaca.org/Pages/default.aspx](https://www.isaca.org/Pages/default.aspx))
- Cloud Security Alliance ([https://cloudsecurityalliance.org/](https://cloudsecurityalliance.org/))
54151HACS Labor Categories

TTK-21.2 Cybersecurity Technical Writer

The **Cybersecurity Technical Writer** helps TalaTek achieve the highest level of customer satisfaction by delivering consistently high-quality cybersecurity work products. Our team has customer satisfaction as a primary quality objective. TalaTek structures our service delivery around “what” service or quality level is required, as opposed to “how” the team should perform the work (i.e., results, not compliance). The objective of the Cybersecurity Technical Writer is to ensure the “what” (work products) meet the customer’s expected outcomes or performance objectives.

The **Cybersecurity Technical Writer** position requires the following abilities:

- Review and update the TalaTek Quality Assurance Surveillance Plan (QASP). The QASP defines work products to be reviewed and the scope and level of review required. The scope of the review may encompass entire documents or may require sampling. Depending on the level of effort, the QASP will specify that reviews check for quality, accuracy, completeness, and compliance with the TalaTek process, as well as compliance with applicable customer process and standards and NIST publication standards.
- Perform scheduled reviews of cybersecurity work products following the QASP. This will include reviewing cybersecurity documents and control analysis produced by TalaTek teams.
- Identify needed improvements in reviewed cybersecurity documents and/or associated process.
- Provide feedback and guidance to document authors/process owner based on above Quality Assurance (QA) review. Feedback will generally include comments in documents and checklists; it may also include tracking changes.
- Perform ad hoc or, as requested, reviews with feedback for quality, accuracy and completeness, documents and control analysis results.
- Review other TalaTek documents related to Business Development, FedRAMP, and other efforts, and provide feedback and guidance.
- Review the overall status of projects and progress to identify omissions and ensure TalaTek processes and customer regulations and policies are following the identified repeatable processes.
- Ensure that defined processes are consistently implemented across all teams/products and service delivery areas. Provide feedback for process improvement, training requirements, or resource allocation based on root cause analysis of identified risk area.
- Coordinate to ensure cybersecurity work products reflect proper grammar, spelling, punctuation, formats, etc.
- Develop metrics for quarterly quality report for presentation to TalaTek and client management.
- Manage day-to-day operational aspects of a documentation and deliverables.
- Prepare deliverables drafted by team before passing to client.
- Effectively applies technical standards to customer deliverables.
- Prepare for engagement reviews and QA procedures.
- Ensure deliverables are complete, current, and stored appropriately.
- Utilize previous experience in the IT risk and/or IT security field to ensure consistency across functional and technical groups.
- Identify, communicate, and manage all deliverable tasks.
- Must possess proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership.
- Education/Experience: Bachelor’s degree in a relevant field or equivalent is preferred and seven (7) years of IT and/or cybersecurity experience.
The **Cybersecurity Technical Writer** will:

- Build the annual QASP. The QASP will identify:
  - Work products to be reviewed,
  - Schedule for review,
  - Type and level of review required, and
  - Standards against which the work products will be measured.

- Analyze work products according to the QASP.

- When reviewing the analysis of NIST controls, the Cybersecurity Technical Writer will consider:
  - Is analysis complete and up to date?
  - Has the analysis addressed NIST and client requirements adequately?
  - Does the analysis support the conclusion?
  - Has evidence been supplied to support the conclusion?
  - Does the analysis comply with TalaTek procedures?

- When reviewing System Security Plans; Risk Assessments; client Risk Acceptances; Privacy Impact Assessment (PIA); Program Security Categorization; quarterly status reports to the AO, ISSO, and CISO, and an annual update to the AO; and other client-required documents, the Cybersecurity Technical Writer will consider:
  - Project plans
  - TalaTek procedures
  - Client requirements, policies, procedures, standards, and processes
  - NIST publications

- Provide client support and attend meetings as needed.

- Advise project managers and TalaTek staff on needed changes to TalaTek policies and procedures based on the results of the QA process.

- Develop and implement new processes based on changes to the TalaTek QASP.

**Expectations** – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing work products, documents, and deliverables.
- Be capable of communicating complex issues efficiently, effectively, and diplomatically to peers, TalaTek leadership, and clients.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

**Requirements** – The **Cybersecurity Technical Writer** will, at minimum, have:

- Bachelor’s degree in Computer Information Systems or equivalent is preferred and seven (7) years of experience in IT and/or cybersecurity
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing Training requirements of the **Cybersecurity Technical Writer**:

- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Pursue ongoing research and training associated with being informed and aware of current organizational QA best practices.
• Utilize training and information resources, which include:
  o The American Society for Quality (http://asq.org/knowledge-center/index.html)
  o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  o American Association for Laboratory Accreditation (https://www.a2la.org/index.cfm)
TTK-22.2 Cybersecurity Project Manager

The TalaTek Cybersecurity Project Manager role requires a project management professional with a proven approach for rapidly moving organizations to a culture of disciplined planning and execution of strategic cybersecurity projects and programs. The TalaTek Cybersecurity Project Manager possesses past experience in a range of practical environments with a proven record of services and delivery of cybersecurity project management. The Cybersecurity Project Manager's role is to stay on top of all aspects of the TalaTek cybersecurity project: process, interpersonal, and organizational and to forge a spirit of cooperation and achievement among the diverse team members. The Cybersecurity Project Manager is expected to deal effectively with all the contingencies, foreseen and unforeseen, ensuring delivery on budget and according to timeline set by customer.

The Cybersecurity Project Manager will:

• Create and execute cybersecurity project work plans and revise as appropriate to meet changing client needs and requirements.
• Manage day-to-day operational aspects of a cybersecurity project and scope.
• Review deliverables prepared by team before passing to client.
• Effectively apply our methodology and enforce project standards.
• Prepare for engagement reviews and QA procedures.
• Minimize TalaTek and TalaTek client exposure and risk on cybersecurity projects.
• Ensure project documents are complete, current, and stored appropriately.
• Utilize previous experience working in IT risk and/or cybersecurity to ensure consistency across functional and technical groups.
• Build and maintain a good working relationship with the client and team members.
• Effectively communicate to TalaTek leadership, project teams, clients, and supporting organizations to ensure expectations are known and consistently managed.
• Identify, communicate, and manage all project risks.

Expectations – The successful candidate will:

• Work independently with minimal supervision.
• Know how to seek out guidance/assistance from appropriate resources when necessary.
• Apply great attention to detail when reviewing work products, documents, and deliverables.
• Be capable of communicating complex issues efficiently, effectively, and diplomatically to peers, TalaTek leadership, and clients.
• Multitask effectively.
• Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Cybersecurity Project Manager will, at minimum, have:

• Project Management Professional (PMP) certification (recommended)
• Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership
• Proficiency in Microsoft Project
• Bachelor's degree in Computer Information Systems or equivalent is preferred and four (4) years of experience in IT and/or cybersecurity Project Management

Ongoing Training requirements of the Cybersecurity Project Manager:

• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Pursue ongoing research and training associated with being informed and aware of up-to-date project management best practices.

• Utilize training and information resources, which include:
  o Project Management Institute (http://www.pmi.org/en.aspx)
  o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  o American Association for Laboratory Accreditation (https://www.a2la.org/index.cfm)
TTK-22.3 Cybersecurity Program Manager

The TalaTek **Cybersecurity Program Manager** role requires a project management professional with a proven approach for rapidly moving organizations to a culture of disciplined planning and execution of multiple strategic cybersecurity projects and programs. The TalaTek Cybersecurity Program Manager possesses past experience in a range of practical environments with a proven record of services and delivery of multiple concurrent cybersecurity project management contracts. The Cybersecurity Program Manager’s role is to stay on top of all aspects of TalaTek cybersecurity projects: process, interpersonal, and organizational and to forge a spirit of cooperation and achievement among the diverse teams and team members. The Cybersecurity Program Manager is expected to deal effectively with all the contingencies, foreseen and unforeseen, ensuring delivery on budget and according to timeline set by customer for all projects.

The **Cybersecurity Program Manager** will:

- Create and execute cybersecurity project work plans and revise as appropriate to meet changing client needs and requirements.
- Manage day-to-day operational aspects of multiple cybersecurity projects and scopes.
- Review deliverables prepared by teams before passing to client.
- Effectively apply our methodology and enforce program and project standards.
- Prepare for engagement reviews and QA procedures.
- Minimize TalaTek and TalaTek client exposure and risk across cybersecurity projects.
- Ensure project documents are complete, current, and stored appropriately.
- Utilize previous experience working in IT risk and/or cybersecurity to ensure consistency across functional and technical groups.
- Build and maintain a good working relationship with clients and teams.
- Effectively communicate to TalaTek leadership, project teams, clients, and supporting organizations to ensure expectations are known and consistently managed.
- Identify, communicate, and manage all projects’ risks.

**Expectations** – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing work products, documents, and deliverables.
- Be capable of communicating complex issues efficiently, effectively, and diplomatically to peers, TalaTek leadership, and clients.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

**Requirements** – The **Cybersecurity Program Manager** will, at minimum, have:

- Project Management Professional (PMP) certification (recommended)
- Proficient written and verbal communication skills in order to effectively interact with clients, project teams, and TalaTek leadership
- Proficiency in Microsoft Project
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and eight (8) years of experience in IT and/or cybersecurity Program Management

Ongoing Training requirements of the **Cybersecurity Program Manager**:

- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Pursue ongoing research and training associated with being informed and aware of up-to-date project management best practices.

• Utilize training and information resources, which include:
  - Project Management Institute (http://www.pmi.org/en.aspx)
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  - American Association for Laboratory Accreditation (https://www.a2la.org/index.cfm)
TTK-23.2 Deputy Cybersecurity Quality System Manager

The Deputy Cybersecurity Quality System Manager possesses past experience ensuring the maintenance of cybersecurity Quality Systems. The Deputy Cybersecurity Quality System Manager must be able to communicate effectively with the Cybersecurity Quality System Manager on all matters related to the performance of the cybersecurity Quality System and report areas needing improvement. Additionally, the Deputy Cybersecurity Quality System Manager is expected to deal effectively with all contingencies and assist the Cybersecurity Quality System Manager with the delivery of a cybersecurity Quality System as outlined in the Quality System Manual. In the absence of the Cybersecurity Quality System Manager, the Deputy Cybersecurity Quality System Manager shall ensure the maintenance of a cybersecurity Quality System in accordance with ISO/IEC 17020:2012, Conformity assessment—Requirements for the operation of various types of bodies performing inspection.

The Deputy Cybersecurity Quality System Manager will:

• Assist with ensuring that all processes needed for the cybersecurity Quality System are established, implemented, and maintained.
• Report to the Cybersecurity Quality System Manager on the performance of the cybersecurity Quality System and any changes needed for improvement.
• Assist the Cybersecurity Quality System Manager in communicating with external assessment bodies on all matters related to the external accreditation process.
• Ensure that a document control procedure is adopted to approve, review, and update all changes to critical documents within the scope of the cybersecurity Quality System.
• Establish and maintain records to be provided as evidence that the cybersecurity Quality System is being followed and that there is a system in place for the identification, storage, protection, retrieval, retention time, and disposal of such records.
• Track the review of the cybersecurity Quality System and ensure that the review is conducted on planned intervals to ensure its continuing suitability, adequacy, and effectiveness. This review includes assessing opportunities for improvement and the need for changes to the cybersecurity Quality System.
• Induct all new TalaTek team members into the requirements of the cybersecurity Quality System related to their roles and responsibilities. Provide update trainings as necessary.
• Ensure that all suppliers used by TalaTek are selected and evaluated/re-evaluated and that records of this assessment are maintained.
• Conduct internal audits of the cybersecurity Quality System in accordance with ISO 17020:2012, verifying that the cybersecurity Quality System conforms to planned internal audit arrangements and is effectively implemented and maintained, and taking appropriate action to identify when this is not the case.
• Contribute to continual improvements to the cybersecurity Quality System, ensuring that evidence of corrective and preventative actions taken are recorded and reviewed.

Expectations – The successful candidate will:

• Work independently with minimal supervision.
• Know how to seek out guidance/assistance from appropriate resources when necessary.
• Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
• Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
• Keep abreast of the latest technologies.
• Multitask effectively.
• Capitalize on strengths and identify areas of opportunities for improvement.
Requirements – Deputy Cybersecurity Quality System Manager will, at a minimum, have:

- Training on ISO 17020:2012, Conformity assessment – Requirements for the operation of various types of bodies performing inspection. (recommended)
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, cybersecurity Quality System Manager, and TalaTek leadership
- Bachelor's degree in Computer Information Systems or equivalent is preferred and four (4) years of experience in IT and/or cybersecurity.

Ongoing Training requirements of the Deputy Cybersecurity Quality System Manager:

- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Pursue ongoing research and training associated with being informed and aware of current organizational quality assurance best practices.
- Utilize training and information resources, which include:
  - The American Society for Quality (http://asq.org/knowledge-center/index.html)
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  - American Association for Laboratory Accreditation (https://www.a2la.org/index.cfm)
TTK-23.3 Cybersecurity Quality System Manager

The TalaTek Cybersecurity Quality System Manager possesses past experience ensuring the development and maintenance of cybersecurity Quality Systems. The Cybersecurity Quality System Manager must be able to communicate effectively on all matters related to the performance of the cybersecurity Quality System and report areas needing improvement. Additionally, the Cybersecurity Quality System Manager is expected to deal effectively with all contingencies (both internal and external), foreseen and unforeseen, and ensuring delivery of a cybersecurity Quality System as outlined in the Quality System Manual. The Cybersecurity Quality System Manager shall ensure the maintenance of a cybersecurity Quality System in accordance with ISO/IEC 17020:2012, Conformity assessment—Requirements for the operation of various types of bodies performing inspection.

The Cybersecurity Quality System Manager will:

- Ensure that processes needed for the cybersecurity Quality System are established, implemented, and maintained.
- Report to top management on the performance of the cybersecurity Quality System and any changes needed for improvement.
- Ensure the promotion of customer requirements throughout TalaTek.
- Liaise with external assessment bodies on all matters related to the external accreditation process.
- Ensure that a document control procedure is adopted and followed to approve, review, and update all changes to critical documents within the scope of the cybersecurity Quality System.
- Establish and maintain records to be provided as evidence that the cybersecurity Quality System is being followed and that there is a system in place for the identification, storage, protection, retrieval, retention time, and disposal of such records.
- Track the review of the cybersecurity Quality System and ensure that the review is conducted on planned intervals to ensure its continuing suitability, adequacy, and effectiveness. This review includes assessing opportunities for improvement and the need for changes to the cybersecurity Quality System.
- Ensure that cybersecurity Quality System Objectives are set by TalaTek senior management for measuring the performance of the cybersecurity Quality System and that these measures are regularly reviewed.
- Induct all new TalaTek team members into the requirements of the cybersecurity Quality System related to their roles and responsibilities. Provide update trainings as necessary.
- Ensure that all suppliers used by TalaTek are selected and evaluated/re-evaluated and that records of this assessment are maintained.
- Manage the implementation and maintenance of the TalaTek ISO 17020:2012 internal audit program, verifying that the cybersecurity Quality System conforms to planned internal audit arrangements and is effectively implemented and maintained, and taking appropriate action to identify when this is not the case.
- Analyze data relating to the effectiveness of the cybersecurity Quality System and evaluate on a continuous basis where improvements to the cybersecurity Quality System can be made based on the findings from the analysis. This can also include data generated as a result of monitoring and measurement from other relevant external sources.
- Coordinate continual improvements to the cybersecurity Quality System, ensuring that evidence of corrective and preventative actions taken are recorded and reviewed.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
• Keep abreast of the latest technologies.
• Multitask effectively.
• Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Cybersecurity Quality System Manager will, at a minimum, have:
• Training on ISO 17020:2012, Conformity assessment – Requirements for the operation of various types of bodies performing inspection. (recommended)
• Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership
• Bachelor’s degree in Computer Information Systems or equivalent is preferred and seven (7) years of experience in IT and/or cybersecurity

Ongoing Training requirements of the Cybersecurity Quality System Manager:
• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Pursue ongoing research and training associated with being informed and aware of current organizational quality assurance best practices.
• Utilize training and information resources, which include:
  o The American Society for Quality (http://asq.org/knowledge-center/index.html)
  o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  o American Association for Laboratory Accreditation (https://www.a2la.org/index.cfm)
TTK-24.3 Senior Information Cybersecurity Consultant

The Senior Information Cybersecurity Consultant possesses past experience in a range of practical environments with a proven record of services and delivery of IT project management. The Senior Information Cybersecurity Consultant will ensure effective delivery of the overall Cybersecurity Assessment process according to NIST SP 800-37. Additionally, the Senior Information Cybersecurity Consultant is expected to deal effectively as a Project Manager role with all contingencies, foreseen and unforeseen, and ensuring delivery on or under budget and according to the timeline set by the customer.

The Senior Information Cybersecurity Consultant will:

- Manage all SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop and complete risk assessments based on NIST standards to ensure the Information Assurance (IA) design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology; supervise other team members to complete project requirements effectively.
- Identify, document, and report cybersecurity issues and concerns to officials; follow up on action items to resolve cybersecurity issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Perform the technical cybersecurity architect role, creating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for cybersecurity incident monitoring, audit and logging procedures for enhancing the client’s infrastructure cybersecurity (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Required to carry out all inspections in accordance with ISO/IEC 17020:2012, Conformity assessment – Requirements for the operation of various types of bodies performing inspection.
- Support and provide in-depth understanding of the TalaTek process and the ability to implement action items, manage reports, and provide overall systems support.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Expectations – a successful candidate will:

- Work independently to optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, and key management tools, etc.).
- Lead the team in conducting cybersecurity risk assessments, vector attack, and penetration testing, and vulnerability assessments of networks and resources attached to the network.
- Identify, document, and report cybersecurity issues and concerns to officials, and follow up on action items to resolve cybersecurity issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Perform the technical cybersecurity architect role, creating design documents and instructional materials for non-security focused teams, detail technical solutions and processes for cybersecurity incident monitoring, audit and logging procedures for enhancing the client’s infrastructure cybersecurity (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, and key management tools, etc.).
Requirements – The Senior Information Cybersecurity Consultant will, at minimum, have:

- CISSP certification, or can attain within six (6) months of hire
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and six (6) years of experience in Information Security
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing training requirements of the Senior Information Cybersecurity Consultant:

- Progressively pursue EC-Council certifications, such as Certified Ethical Hacker (CEH), Licensed Penetration Tester, etc. – order of certifications obtained should be determined based on an ongoing evaluation of candidate’s skills assessments.
- Pursue ongoing research and training associated with being informed and aware of up-to-date cybersecurity best practices and the tools associated with completing cybersecurity assessments – completing vendor-specific training as necessary, such as Qualys, Nessus, etc.
- Maintain Continuing Professional Education (CPE) requirements associated with cybersecurity and/or project management certifications.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloud.cio.gov/fedramp)
  - Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  - International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  - Project Management Institute (http://www.pmi.org/en.aspx)
  - Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-25.1 Junior Cybersecurity Continuous Monitoring Analyst

The **Junior Cybersecurity Continuous Monitoring Analyst** is an entry-level position requiring the following abilities:

- Support SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop cybersecurity risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
- Identify, document, and report cybersecurity issues and concerns to TalaTek leadership and officials.
- Follow up on action items to resolve IT and program cybersecurity issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support the technical cybersecurity architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for cybersecurity incident monitoring, audit and logging procedures for enhancing the client's infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

The **Junior Cybersecurity Continuous Monitoring Analyst** will:

- Support the development of annual Continuous Monitoring Plans.
- Analyze controls each quarter according to plan, following TalaTek processes and workflows as required, in a timely manner. Controls analysis will be phased through the quarter. Analyzing status includes:
  - Is analysis complete and accurate?
  - Does ISO or ISSO have additional requirements?
  - Are there new NIST or industry requirements?
  - Request new or renewed evidence or confirmation of practice for current continuous monitoring period.
  - Analyze new information provided; responding to evidence provided by the client within three (3) working days.
  - Document decisions regarding implementation/compliance status.
  - Update centralized repository to reflect compliance status and attaching evidence supporting decisions.
  - Read and answer all work e-mails within one (1) working day.
  - Support preparation of client-required documentation:
    - Meeting status agenda and minutes
    - Controls and POA&Ms under review report
    - Attend client status meetings and TalaTek status meetings
    - Update central repository with results of the meetings within two (2) working days after the working meeting
    - Update System Security Plan (SSP) and updated Risk Assessment (RA) on schedule
    - Review/revision of the Privacy Impact Assessment (PIA)
    - Review/revision of the Program Security Categorization
    - Provide an updated POA&M report as needed
TalaTek monthly status reports
o Quarterly status reports to the AO, ISSO, and CISO, and an annual update to the AO
o Annual review and renewals of Risk Acceptances for risk-based decisions
o Annual year-end review
o Other client-required documents

• Provide onsite (client) support and attend meetings as needed.
• Respond to audit requests and findings.
  o Supply documents requested by auditor

• Conduct onsite visits to client site(s) for:
  o Security control and documentation review
  o Site inspections

• Create White Papers on security topics as needed for TalaTek/client.
• Support internal QA efforts on an ongoing basis.
• Develop and implement new processes based on changes to TalaTek, client and/or NIST requirements.

Expectations – The successful candidate will:

• Work independently with minimal supervision.
• Know how to seek out guidance/assistance from appropriate resources when necessary.
• Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
• Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
• Keep abreast of the latest technologies.
• Multitask effectively.
• Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Junior Cybersecurity Continuous Monitoring will, at minimum, have:

• CompTIA Security+ certification within one (1) to two (2) years of beginning employment at TalaTek (recommended)
• Aptitude for processing complex IT and/or cybersecurity concepts
• Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership
• Bachelor’s degree in Computer Information Systems or equivalent is preferred and two (2) years of experience in Information Security and/or cybersecurity

Ongoing Training requirements of the Junior Cybersecurity Continuous Monitoring Analyst:

• Progressively pursue (ISC)^2 and ISACA certifications, such as Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA), etc. – order of certifications obtained should be determined based on ongoing evaluation of candidate’s skills assessments.
• Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results of ongoing observations and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.

• Utilize training and information resources, which include:
  o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  o FedRAMP (http://cloud.cio.gov/fedramp)
  o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  o International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  o Project Management Institute (http://www.pmi.org/en.aspx)
  o Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-25.2 Cybersecurity Continuous Monitoring Analyst

Information Security Continuous Monitoring (ISCM) is a team effort. The team consists of a Cybersecurity Project Manager, Cybersecurity Control Analysts, and Cybersecurity Quality Control personnel. Cybersecurity Analysts are responsible for ongoing monitoring of specific families of controls. Cybersecurity Analysts monitor the control families to reflect the current status of controls in near real-time. The Cybersecurity Continuous Monitoring Analyst is a mid-level position requiring the following abilities:

- Manage a team, as described above, to achieve client/task goals, deadlines, and risk management objectives, and report to senior management on cybersecurity issues and progress, as well as make recommendations for process improvement.
- Be part of the ISCM team, involved in all tasks, and with experience providing: project planning, guidance, mentoring, and support to the various roles within the team, such as Project Manager QA and Cybersecurity Analysts.

The Cybersecurity Continuous Monitoring Analyst will:

- Develop and support the implementation of the annual ISCM Plan.
- Supervise and provide subject matter expertise for control analysis each quarter according to the ISCM Plan, following TalaTek processes in a timely manner. Control analysis will be phased throughout the quarter, with initial analysis of all controls completed within 45 days after the quarter starts.
- Provide QA for control analysis accuracy and level of detail in context of the system’s risk and categorization:
  - Was previous analysis complete and accurate?
  - Does ISO/IO or ISSO have additional requirements?
  - Are there new organizational or NIST requirements?
  - Are there related controls or POA&M items that need to be addressed?
  - Understand the concept of inherited controls, common control providers, and assess risks accordingly.
- Ensure collection of new or renewed evidence and confirm that supporting evidence for control analysis is accurate and meets security standards.
- Analyze new information provided and respond to evidence collected within three (3) working days.
- Responsible for final document decisions regarding implementation/compliance status.
- Make sure cybersecurity controls status is up to date and reflects compliance status, and attach evidence supporting the decision.
- Read and answer emails within one (1) working day.
- Support preparation of client-required documents:
  - Bi-weekly status agenda and minutes
  - Bi-weekly controls and POA&Ms under review report
  - Attend client bi-weekly status meetings and TalaTek weekly status meetings
  - Update related systems with results of the meetings within two (2) working days after the TalaTek working meeting (this includes entering comments, updating status, attaching documents)
  - Update the System Security Plan (SSP) and Risk Assessment (RA)
  - Review/revision of the Privacy Impact Assessment (PIA) and PTA, if needed
  - Review/revision of the Program Security Categorization consistent with FIPS 199
  - Provide an updated POA&M report each quarter with up-to-date Recommended Actions for each outstanding POA&M
  - Monthly status reports
  - Quarterly status reports to the AO, ISSO, and CISO, and annual update to the AO
  - Annual review and renewals of Risk Acceptances
  - Annual year-end review
Authorized Multiple Award Schedule Catalog/Price List
Contract Number: GS-35F-399DA

- Other required documents (i.e., Classification and Determination memo, PIA Executive Summary, Bi-annual Cycle memo, etc.)
- At a minimum, provide onsite (client) support one (1) day per week for meetings as needed.
- Read and answer emails from client quickly on the same day, if possible.
- Respond to audit requests and findings.
- Supply documents requested by auditor.
- Prepare Request for Closure of Findings (RCFs) and related documents.
- Conduct onsite visits to client sites, if needed, for:
  - Document review
  - Site inspections
- Create White Papers on security topics as needed.
- Perform internal QA.
- Develop and implement new processes based on changes to client and/or NIST requirements.
- Support TalaTek new business research and proposals, as needed.
- Respond to other requests as needed.

**Expectations** – The successful candidate will:
- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients. Immediately acknowledge that requests were received, provide a quick response to requests, and deliver a very professional level of product.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

**Requirements** – The **Cybersecurity Continuous Monitoring Analyst** will, at minimum, have:
- Bachelor's degree in Computer Information Systems or equivalent is preferred and four (4) years of IT experience in Information Systems and/or cybersecurity
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing Training requirements of the **Cybersecurity Continuous Monitoring Analyst**:
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results on ongoing observation and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology [http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)
Authorized Multiple Award Schedule Catalog/Price List
Contract Number: GS-35F-399DA

- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
- Project Management Institute (http://www.pmi.org/en.aspx)
- Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-25.3 Senior Cybersecurity Continuous Monitoring Analyst

The Senior Cybersecurity Continuous Monitoring Analyst is a senior-level position requiring the following abilities:

• Manage SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
• Develop cybersecurity risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risks.
• Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
• Identify, document, and report cybersecurity issues and concerns to officials.
• Follow up on action items to resolve IT and program cybersecurity issues.
• Develop remediation plans and coordinate activities with other organizational departments.
• Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
• Support the technical cybersecurity architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
• Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

The Senior Cybersecurity Continuous Monitoring Analyst will:

• Build annual Continuous Monitoring Plans.
• Analyze controls each quarter according to plan, following TalaTek processes and workflows, as required, in a timely manner. Controls analysis will be phased through the quarter. Analyzing status includes:
  o Is analysis complete and accurate?
  o Does ISO or ISSO have additional requirements?
  o Are there new NIST or industry requirements?
• Request new or renewed evidence or confirmation of practice for current continuous monitoring period.
• Analyze new information provided; respond to evidence provided by the client within three (3) working days.
• Document decisions regarding implementation/compliance status.
• Update centralized repository to reflect compliance status and attaching evidence supporting decisions.
• Read and answer all work e-mails within one (1) working day.
• Support preparation of client-required documentation:
  o Meeting status agenda and minutes
  o Controls and POA&Ms under review report
  o Attend client status meetings and TalaTek status meetings
  o Update central repository with results of the meetings within two (2) working days after the working meeting
  o Updated System Security Plan (SSP) and updated Risk Assessment (RA) on schedule
  o Review/revision of the Privacy Impact Assessment (PIA)
  o Review/revision of the Program Security Categorization
• Provide an updated POA&M report as needed
• TalaTek monthly status reports
• Quarterly status reports to the AO, ISSO, and CISO, and an annual update to the AO
• Annual review and renewals of Risk Acceptances for risk-based decisions
• Annual year-end review
• Other client-required documents

• Provide onsite (client) support and attend meetings as needed.
• Respond to audit requests and findings.
  o Supply documents requested by auditor
• Conduct onsite visits to client site(s) for:
  o Security control and documentation review
  o Site inspections
• Create White Papers on security topics as needed for TalaTek/client.
• Perform internal QA on an ongoing basis.
• Develop and implement new processes based on changes to TalaTek, client, and/or NIST requirements.

Expectations – The successful candidate will:
• Work independently with minimal supervision.
• Know how to seek out guidance/assistance from appropriate resources when necessary.
• Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
• Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
• Keep abreast of the latest technologies.
• Multitask effectively.
• Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Senior Cybersecurity Continuous Monitoring will, at minimum, have:
• CISSP certification and continuing related professional development, or can attain within six (6) months of hire (recommended)
• Bachelor’s degree in Computer Information Systems or equivalent is preferred and eight (8) years of IT experience in Information Systems and/or cybersecurity
• Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing Training requirements of the Senior Cybersecurity Continuous Monitoring Analyst:
• Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results on ongoing observation and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
• Utilize training and information resources, which include:
  o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  o FedRAMP (http://cloud.cio.gov/fedramp)
- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
- Project Management Institute (http://www.pmi.org/en.aspx)
- Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-26.2 Cybersecurity Analyst

The Cybersecurity Analyst will:

- Manage SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Identify, document, and report security issues and concerns to officials.
- Follow up on action items to resolve IT and program security issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes, including the following tasks:
  - Analyzing vulnerability reports (Qualys or Nessus related data)
  - Analyzing audit logs (Splunk)
  - Creating actionable reports of findings to be provided to customers
  - Using anti-spam/anti-spyware tools
  - Applying knowledge of enterprise configuration and integrity management tools
- Manage a team to achieve client/task goals, deadlines, risk management and objectives, and report to senior management on issues, progress, and recommendations for process improvement.
- Mentor team members and provide training and expertise.
- Evaluate new equipment and methodologies and provide reviews and recommendations.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Cybersecurity Analyst will, at minimum, have:

- CISSP certification and continuing related professional development, or obtain within six (6) months of hire (recommended)
- CEH, CCSK, AWS Architect, and/or other related certifications, or obtain within six (6) months of hire (recommended)
- Proficient written and verbal communication skills
- Experience with interdisciplinary areas such as Systems Engineering and Software integration
- Bachelor’s degree or equivalent is preferred and seven (7) years of IT experience in Information Security

Ongoing Training requirements of the Cybersecurity Analyst:

- Progressively pursue (ISC)² and ISACA certifications, such as Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA), etc. – order of certifications obtained should be determined based on ongoing evaluation of candidate’s skills assessments.
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results of ongoing observations and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
• Utilize training and information resources, which include:
  o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  o FedRAMP (http://cloud.cio.gov/fedramp)
  o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  o International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  o Project Management Institute (http://www.pmi.org/en.aspx)
  o Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-26.3 Senior Cybersecurity Analyst

The Senior Cybersecurity Analyst will:

- Supervise and provide subject matter expertise for SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Identify, document, and report security issues and concerns to officials.
- Follow up on action items to resolve IT and program security issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes, including the following tasks:
  - Analyzing vulnerability reports (Qualys or Nessus related data)
  - Analyzing audit logs (Splunk)
  - Creating actionable reports of findings to be provided to customers
  - Using anti-spam/anti-spyware tools
  - Applying knowledge of enterprise configuration and integrity management tools
- Supervise and provide subject matter expertise for a team to achieve client/task goals, deadlines, risk management and objectives, and report to senior management on issues, progress, and recommendations for process improvement.
- Mentor team members and provide training and expertise.
- Evaluate new equipment and methodologies and provide reviews and recommendations.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The Senior Cybersecurity Analyst will, at minimum, have:

- CISSP certification and continuing related professional development, or obtain within six (6) months of hire (recommended)
- CEH, CCSK, AWS Architect, and/or other related certifications, or obtain within six (6) months of hire (recommended)
- Proficient written and verbal communication skills
- Experience with interdisciplinary areas such as Systems Engineering and Software integration
- Bachelor’s degree or equivalent is preferred and eight to ten (8-10) years of IT experience in Information Security

Ongoing Training requirements of the Senior Cybersecurity Analyst:

- Progressively pursue (ISC)² and ISACA certifications, such as Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA), etc. – order of certifications obtained should be determined based on ongoing evaluation of candidate’s skills assessments.
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications

Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results of ongoing observations and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.

Utilize training and information resources, which include:

- National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
- FedRAMP (http://cloud.cio.gov/fedramp)
- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
- Project Management Institute (http://www.pmi.org/en.aspx)
- Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-27.2 Information Cybersecurity Analyst

The **Information Cybersecurity Analyst** is a mid-level position requiring the following abilities:

- Conduct SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop cybersecurity risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
- Identify, document, and report cybersecurity issues and concerns to officials.
- Follow up on action items to resolve IT and program cybersecurity issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support the technical cybersecurity architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

**Expectations** – a successful candidate will:

- Work independently to optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, and key management tools, etc.).
- Work with a team to conduct security risk assessments, vector attack, and penetration testing, and vulnerability assessments of networks and resources attached to the network.
- Identify, document, and report security issues and concerns to officials, and follow up on action items to resolve security issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Perform the technical security architect role, creating design documents and instructional materials for non-security focused teams, detail technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, and key management tools, etc.).

**Requirements** – The **Information Cybersecurity Analyst** will, at minimum, have:

- CISSP certification, or can attain within six (6) months of hire
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and three (3) years of experience in Information Security
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing training requirements of the **Senior Information Security Analyst**:

- Progressively pursue EC-Council certifications, such as Certified Ethical Hacker (CEH), Licensed Penetration Tester, etc. – order of certifications obtained should be determined based on an ongoing evaluation of candidate’s skills assessments.
Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and the tools associated with completing security assessments – completing vendor-specific training as necessary, such as Qualys, Nessus, etc.

Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.

Utilize training and information resources, which include:

- National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
- FedRAMP (http://cloud.cio.gov/fedramp)
- Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
- International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
- Project Management Institute (http://www.pmi.org/en.aspx)
- Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-27.3 Senior Information Cybersecurity Analyst

The Senior Information Cybersecurity Analyst is a senior-level position requiring the following abilities:

- Manage SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop cybersecurity risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
- Identify, document, and report cybersecurity issues and concerns to officials.
- Follow up on action items to resolve IT and program cybersecurity issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support the technical cybersecurity architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

Expectations – a successful candidate will:

- Work independently to optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, and key management tools, etc.).
- Lead the team in conducting security risk assessments, vector attack, and penetration testing, and vulnerability assessments of networks and resources attached to the network.
- Identify, document, and report security issues and concerns to officials, and follow up on action items to resolve security issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Perform the technical security architect role, creating design documents and instructional materials for non-security focused teams, detail technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, and key management tools, etc.).

Requirements – The Senior Information Cybersecurity Analyst will, at minimum, have:

- CISSP certification, or can attain within six (6) months of hire
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and five (5) years of experience in Information Security
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing training requirements of the Senior Information Cybersecurity Analyst:

- Progressively pursue EC-Council certifications, such as Certified Ethical Hacker (CEH), Licensed Penetration Tester, etc. – order of certifications obtained should be determined based on an ongoing evaluation of candidate’s skills assessments.
• Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and the tools associated with completing security assessments – completing vendor-specific training as necessary, such as Qualys, Nessus, etc.
• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Utilize training and information resources, which include:
  o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  o FedRAMP (http://cloud.cio.gov/fedramp)
  o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  o International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  o Project Management Institute (http://www.pmi.org/en.aspx)
  o Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-28.2 Cybersecurity Control Assessor

The Cybersecurity Control Assessor is a senior-level position requiring the following abilities:

- Manage SA&A tasks across multiple systems and ensure NIST publication standards are applied effectively and consistently.
- Develop cybersecurity risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
- Identify, document, and report cybersecurity issues and concerns to officials.
- Follow up on action items to resolve IT and program cybersecurity issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support the technical cybersecurity architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

Expectations – a successful candidate will:

- Work independently to optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, and key management tools, etc.).
- Lead the team in conducting security risk assessments, vector attack, and penetration testing, and vulnerability assessments of networks and resources attached to the network.
- Identify, document, and report security issues and concerns to officials, and follow up on action items to resolve security issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Perform the technical security architect role, creating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, and key management tools, etc.).

Requirements – The Cybersecurity Control Assessor will, at minimum, have:

- CISSP certification, or can attain within six (6) months of hire
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and four (4) years of experience in Information Security
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing training requirements of the Cybersecurity Control Assessor:

- Progressively pursue EC-Council certifications, such as Certified Ethical Hacker (CEH), Licensed Penetration Tester, etc. – order of certifications obtained should be determined based on an ongoing evaluation of candidate’s skills assessments.
• Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and the tools associated with completing security assessments – completing vendor-specific training as necessary, such as Qualys, Nessus, etc.
• Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
• Utilize training and information resources, which include:
  o National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  o FedRAMP (http://cloud.cio.gov/fedramp)
  o Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  o International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  o Project Management Institute (http://www.pmi.org/en.aspx)
  o Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-29.1 Junior Cybersecurity Vulnerability Analyst

The Junior Cybersecurity Vulnerability Analyst will:

- Under senior supervision, perform cybersecurity Penetration Assessments exploiting and compromising defined targets in enterprise environments ranging from web applications to handheld systems.
- Under senior supervision, perform penetration testing on organizational information systems using both automated tools and manual methods to exploit identified weaknesses in applications, systems, and networks.
- Under senior supervision, identify and exploit vulnerabilities in web and mobile applications, OS, hardware, databases, wired and wireless networks, etc.
- Under senior supervision, identify, investigate, analyze, and remediate information security events to ensure enterprise integrity against technical and physical risks.
- Under senior supervision, conduct extensive research and capitalize on experience and skills to craft new exploitations, stress systems to achieve nonstandard responses, and breach authorization boundaries.
- Mimic threat adversary capabilities, tactics, techniques, and procedures to attain information disclosure, root/administrative access, or other exploitation success.
- Under senior supervision, conduct technical and physical social engineering activities to obtain unauthorized information disclosure while identifying human error and weakness in an organization.
- Under senior supervision, conduct technical and physical social engineering activities to obtain unauthorized information disclosure while identifying human error and weakness in an organization.
- Document technical and logical cybersecurity findings identified during the cybersecurity assessments and providing security recommendations for enterprise executives, developers, web/system and database administrators.
- Under senior supervision, identify, document, and report cybersecurity issues and concerns to officials.
- Follow up on action items to resolve IT and program cybersecurity issues.
- Under senior supervision, develop remediation plans and coordinate activities with other organizational departments.
- Under senior supervision, optimize up-to-date technical solutions and processes, including the following tasks:
  - Analyzing vulnerability reports (e.g., Qualys or Nessus related data)
  - Analyzing audit logs (e.g., Splunk)
  - Creating actionable reports of findings to be provided to customers
  - Using anti-spam/anti-spyware tools
  - Applying knowledge of enterprise configuration and integrity management tools
- Assist the team to achieve client/task goals, deadlines, risk management and objectives, and report to senior management on issues, progress, and recommendations for process improvement.
- Evaluate new equipment and methodologies and provide reviews and recommendations.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.
**Requirements** – The **Junior Cybersecurity Vulnerability Analyst** will, at minimum, have:

- CEH, CCSK, AWS Architect, and/or other related certifications, or obtain within six (6) months of hire (recommended)
- Proficient written and verbal communication skills
- Experience with interdisciplinary areas such as Systems Engineering and Software integration
- Bachelor’s degree or equivalent is preferred and one (1) year of IT experience in Information Security

Ongoing Training requirements of the **Junior Cybersecurity Vulnerability Analyst**:

- Progressively pursue (ISC)² and ISACA certifications, such as Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA), etc. – order of certifications obtained should be determined based on ongoing evaluation of candidate’s skills assessments.
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications

Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results of ongoing observations and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.

- Utilize training and information resources, which include:
  - National Institute of Standards and Technology ([http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html))
  - FedRAMP ([http://cloud.cio.gov/fedramp](http://cloud.cio.gov/fedramp))
  - Information Systems Audit and Control Association ([https://www.isaca.org/Pages/default.aspx](https://www.isaca.org/Pages/default.aspx))
  - Cloud Security Alliance ([https://cloudsecurityalliance.org/](https://cloudsecurityalliance.org/))
TTK-30.1 3PAO Junior Cybersecurity Assessor

Information Security Continuous Monitoring (ISCM) is a team effort. The team consists of a Cybersecurity Project Manager, Cybersecurity Continuous Monitoring Analysts, and Cybersecurity Quality Control personnel. Analysts are responsible for ongoing monitoring of specific families of controls. Cybersecurity Analysts monitor the control families to reflect the current status of controls in near real-time. The 3PAO Junior Cybersecurity Assessor is a mid-level position requiring the following abilities:

- Work within a team, as described above, to achieve client/task goals, deadlines, and risk management objectives, and report to senior management on issues and progress, as well as make recommendations for process improvement.
- Be part of the ISCM team, involved in all tasks, and with experience providing: assessment, guidance, mentoring, and support to the various roles within the team, such as QA and Cybersecurity Analysts.

The 3PAO Junior Cybersecurity Assessor will:

- Develop and support the implementation of the annual ISCM Plan.
- Provide subject matter expertise for cybersecurity control analysis each quarter according to the ISCM Plan, following TalaTek processes in a timely manner. Cybersecurity control analysis will be phased throughout the quarter, with initial analysis of all controls completed within 45 days after the quarter starts.
- Provide QA for cybersecurity control analysis accuracy and level of detail in context of the system's risk and categorization:
  - Was previous analysis complete and accurate?
  - Does ISO/IO or ISSO have additional requirements?
  - Are there new organizational, NIST, or FedRAMP requirements?
  - Are there related controls or POA&M items that need to be addressed?
  - Understand the concept of inherited controls, common control providers, and assess risks accordingly.
- Ensure collection of new or renewed evidence and confirm that supporting evidence for control analysis is accurate and meets security standards.
- Analyze new information provided and respond to evidence collected within three (3) working days.
- Responsible for final document decisions regarding implementation/compliance status.
- Make sure controls status is up to date and reflects compliance status, and attach evidence supporting the decision.
- Read and answer emails within one (1) working day.
- Support preparation of client-required documents:
  - Bi-weekly status agenda and minutes
  - Bi-weekly controls and POA&Ms under review report
  - Attend client bi-weekly status meetings and TalaTek weekly status meetings
  - Update related systems with results of the meetings within two (2) working days after the TalaTek working meeting (this includes entering comments, updating status, attaching documents)
  - Update the System Security Plan (SSP) and Risk Assessment (RA)
  - Review/revision of the Privacy Impact Assessment (PIA) and PTA, if needed
  - Review/revision of the Program Security Categorization consistent with FIPS 199
  - Provide an updated POA&M report each quarter with up-to-date Recommended Actions for each outstanding POA&M
  - Monthly status reports
  - Quarterly status reports to the AO, ISSO, and CISO, and annual update to the AO
  - Annual review and renewals of Risk Acceptances
  - Annual year-end review
**Expectations** – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients. Immediately acknowledge that requests were received, provide a quick response to requests, and deliver a very professional level of product.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

**Requirements** – The 3PAO Junior Cybersecurity Assessor will, at minimum, have:

- Successfully completed mandatory FedRAMP Project Management Organization (PMO) subject matter training
- At least one industry certification from the following list:
  - Cisco Certified Network Associate Security (CCNA Security)
  - Cisco Certified Network Associate Cyber Security Operations (CCNA Cyber Ops)
  - Cybersecurity Analyst (CySA+)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Systems and Network Auditor (GSNA)
  - GIAC Certified Intrusion Analyst (GCIA)
  - Certified Information Systems Auditor (CISA)
  - Certified Information System Security Professional or Associate (CISSP or Associate)
  - Certified Secure Software Lifecycle Professional (CSSLP)
  - Certified Information Systems Security Officer (CISSO)
  - CyberSec First Responder (CFR)
  - CompTIA Advanced Security Practitioner Continuing Education (CASP+ CE)
  - CompTIA Cloud+ (Cloud+)
  - Global Industrial Cyber Security Professional (GICSP)
  - Securing Cisco® Networks with Threat Detection Analysis (SCYBER)
Authorized Multiple Award Schedule Catalog/Price List
Contract Number: GS-35F-399DA

- Bachelor's degree in Computer Information Systems or equivalent is preferred and one (1) year of IT experience in Information Systems and/or cybersecurity
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership

Ongoing Training requirements of the 3PAO Junior Cybersecurity Assessor:

- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results on ongoing observation and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloud.cio.gov/fedramp)
  - Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  - International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  - Project Management Institute (http://www.pmi.org/en.aspx)
  - Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-30.2 3PAO Cybersecurity Penetration Tester

The 3PAO Cybersecurity Penetration Tester will:

- Perform 3PAO Cybersecurity Penetration Assessments exploiting and compromising defined targets in enterprise environments ranging from web applications to handheld systems.
- Perform penetration testing on organizational information systems using both automated tools and manual methods to exploit identified weaknesses in applications, systems, and networks.
- Identify and exploit vulnerabilities in web and mobile applications, OS, hardware, databases, wired and wireless networks, etc.
- Identify, investigate, analyze, and remediate information security events to ensure enterprise integrity against technical and physical risks.
- Conduct extensive research and capitalize on experience and skills to craft new exploitations, stress systems to achieve nonstandard responses, and breach authorization boundaries.
- Mimic threat adversary capabilities, tactics, techniques, and procedures to attain information disclosure, root/administrative access, or other exploitation success.
- Conduct technical and physical social engineering activities to obtain unauthorized information disclosure while identifying human error and weakness in an organization.
- Document technical and logical cybersecurity findings identified during the cybersecurity assessments and providing security recommendations for enterprise executives, developers, web/system and database administrators.
- Supervise and provide subject matter expertise for SA&A tasks across multiple systems and ensure NIST and FedRAMP publication standards are applied effectively and consistently across multiple systems and ensure NIST and FedRAMP publication standards are applied effectively and consistently.
- Identify, document, and report cybersecurity issues and concerns to officials.
- Follow up on action items to resolve IT and program cybersecurity issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes, including the following tasks:
  - Analyzing vulnerability reports (e.g., Qualys or Nessus related data)
  - Analyzing audit logs (e.g., Splunk)
  - Creating actionable reports of findings to be provided to customers
  - Using anti-spam/anti-spyware tools
  - Applying knowledge of enterprise configuration and integrity management tools
- Supervise and provide subject matter expertise for a team to achieve client/task goals, deadlines, risk management and objectives, and report to senior management on issues, progress, and recommendations for process improvement.
- Mentor team members and provide training and expertise.
- Evaluate new equipment and methodologies and provide reviews and recommendations.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.
Requirements – The 3PAO Cybersecurity Penetration Tester will, at minimum, have:

- Successfully completed mandatory FedRAMP Project Management Organization (PMO) subject matter training
- At least one industry certification related directly to penetration testing with hands-on (performance-based) components required for certification from the following list:
  - Cisco Certified Network Professional CCNP / Security
  - CompTIA Advanced Security Practitioner (CASP)
  - Certified Information Systems Security Professional (CISSP)
  - Certified Secure Software Lifecycle Professional (CSSLP)
  - CISSP-Information Systems Security Engineering Professional (CISSP-ISSEP)
  - SANS GIAC Penetration Tester (GPEN)
  - Open Web Application Security Project Penetration Tester (OWASP)
- Proficient written and verbal communication skills
- Experience with interdisciplinary areas such as Systems Engineering and Software integration
- Bachelor’s degree or equivalent is preferred and two (2) years of IT experience in Information Security

Ongoing Training requirements of the 3PAO Cybersecurity Penetration Tester:

- Progressively pursue (ISC)² and ISACA certifications, such as Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA), etc. – order of certifications obtained should be determined based on ongoing evaluation of candidate’s skills assessments.
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.

Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results of ongoing observations and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.

- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloud.cio.gov/fedramp)
  - Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  - International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  - Project Management Institute (http://www.pmi.org/en.aspx)
  - Cloud Security Alliance (https://cloudsecurityalliance.org/)
**TTK-30.3 3PAO Senior Cybersecurity Assessor**

The **3PAO Senior Cybersecurity Assessor** is a senior-level position requiring the following abilities:

- Manage 3PAO cybersecurity assessments across multiple systems and ensure NIST and FedRAMP publication standards are applied effectively and consistently.
- Develop cybersecurity risk assessments based on NIST and FedRAMP standards to ensure IA design sufficiently mitigates IA risks.
- Define and plan procedures relating to securing technology as well as coordinate with other team members and client resources to effectively complete project requirements.
- Identify, document, and report cybersecurity issues and concerns to officials.
- Follow up on action items to resolve IT and program cybersecurity issues.
- Develop remediation plans and coordinate activities with other organizational departments.
- Optimize up-to-date technical solutions and processes to monitor the security of the client’s infrastructure (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support the technical cybersecurity architect role, updating design documents and instructional materials for non-security focused teams, detailing technical solutions and processes for security incident monitoring, audit and logging procedures for enhancing the client’s infrastructure security (firewalls, servers, applications, anti-spam/anti-spyware tools, forensic integrity checking, encryption, key management tools, etc.).
- Support and provide in-depth understanding of the TalaTek methodology and process, as well as implement action items, manage reports, and provide overall support.

The **3PAO Senior Cybersecurity Assessor** will:

- Build annual Continuous Monitoring Plans.
- Analyze cybersecurity controls each quarter according to plan, following TalaTek processes and workflows, as required, in a timely manner. Controls analysis will be phased through the quarter. Analyzing status includes:
  - Is analysis complete and accurate?
  - Does ISO or ISSO have additional requirements?
  - Are there new NIST, FedRAMP, or industry requirements?
- Request new or renewed evidence or confirmation of practice for current continuous monitoring period.
- Analyze new information provided; respond to evidence provided by the client within three (3) working days.
- Document decisions regarding implementation/compliance status.
- Update centralized repository to reflect compliance status and attaching evidence supporting decisions.
- Read and answer all work e-mails within one (1) working day.
- Support preparation of client-required documentation:
  - Meeting status agenda and minutes
  - Controls and POA&Ms under review report
  - Attend client status meetings and TalaTek status meetings
  - Update central repository with results of the meetings within two (2) working days after the working meeting
  - Updated System Security Plan (SSP) and updated Risk Assessment (RA) on schedule
  - Review/revision of the Privacy Impact Assessment (PIA)
  - Review/revision of the Program Security Categorization
  - Provide an updated POA&M report as needed
  - TalaTek monthly status reports
Authorized Multiple Award Schedule Catalog/Price List
Contract Number: GS-35F-399DA

- Quarterly status reports to the AO, ISSO, and CISO, and an annual update to the AO
- Annual review and renewals of Risk Acceptances for risk-based decisions
- Annual year-end review
- Other client-required documents

- Provide onsite (client) support and attend meetings as needed.
- Respond to audit requests and findings.
  - Supply documents requested by auditor

- Conduct onsite visits to client site(s) for:
  - Security control and documentation review
  - Site inspections

- Create White Papers on security topics as needed for TalaTek/client.
- Perform internal QA on an ongoing basis.
- Develop and implement new processes based on changes to TalaTek, client, NIST, and/or FedRAMP requirements.

Expectations – The successful candidate will:
- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The 3PAO Senior Cybersecurity Assessor will, at minimum, have:
- Successfully completed mandatory FedRAMP Project Management Organization (PMO) subject matter training
- CISSP certification and continuing related professional development, or can attain within six (6) months of hire (recommended) and at least one other industry certification from the following list:
  - CompTIA Advanced Security Practitioner (CASP+ CE)
  - GIAC Certified Enterprise Defender (GCED)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Security Leadership (GSLC)
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Certified Cloud Security Professional (CCSP)
  - CISSP-Information Systems Security Architecture Professional (CISSP-ISSAP)
  - CISSP-Information Systems Security Engineering Professional (CISSP-ISSEP)
  - CISSP-Information Systems Security Management Professional (CISSP-ISSMP)
  - CyberSec First Responder (CFR)
  - Certified Chief Information Security Officer (CCISO)
- Bachelor’s degree in Computer Information Systems or equivalent is preferred and five (5) years of IT experience in Information Systems and/or cybersecurity
- Proficient written and verbal communication skills in order to effectively interact with clients, project team, and TalaTek leadership
Ongoing Training requirements of the 3PAO Senior Cybersecurity Assessor:

- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications.
- Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results on ongoing observation and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.
- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloud.cio.gov/fedramp)
  - Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  - International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  - Project Management Institute (http://www.pmi.org/en.aspx)
  - Cloud Security Alliance (https://cloudsecurityalliance.org/)
TTK-31.3 Virtual Chief Information Security Officer – Cybersecurity

The Virtual Chief Information Security Officer – Cybersecurity (vCISO) will:

- Determine IT enterprise information cybersecurity standards.
- Develop and implements information security standards and procedures.
- Provide tactical information security advice and examining the ramifications of new technologies. Ensure that all information systems are functional and secure.
- Develop and maintain business continuity plans, to include Contingency Plans, Disaster Recovery Plans, and Incident Response Plans, as applicable.

Expectations – The successful candidate will:

- Work independently with minimal supervision.
- Know how to seek out guidance/assistance from appropriate resources when necessary.
- Apply great attention to detail when reviewing, updating, and comparing documents and deliverables.
- Be capable of communicating complex cybersecurity issues efficiently and effectively to peers, TalaTek leadership, and clients.
- Keep abreast of the latest cybersecurity technologies.
- Multitask effectively.
- Capitalize on strengths and identify areas of opportunities for improvement.

Requirements – The vCISO will, at minimum, have:

- CISSP certification and continuing related professional development, or obtain within six (6) months of hire (recommended)
- Proficient written and verbal communication skills
- Experience with interdisciplinary areas such as Systems Engineering and Software integration
- Master’s degree or equivalent is preferred and Ten (10) years of IT experience in Information Security

Ongoing Training requirements of the vCISO:

- Progressively pursue (ISC)² and ISACA certifications, such as Certified Information System Security Professional (CISSP), Certified Information System Auditor (CISA), etc. – order of certifications obtained should be determined based on on-going evaluation of candidate’s skills assessments.
- Pursue ongoing research and training associated with being informed and aware of up-to-date security best practices and relevant publications (i.e., NIST, FedRAMP, National Vulnerability Database, etc.).
- Maintain Continuing Professional Education (CPE) requirements associated with security and/or project management certifications

Potential for additional training requirements will be determined on a candidate-by-candidate basis and based on the results of ongoing observations and skills assessments – training determinations to be discussed between TalaTek leadership and the candidate during annual skills assessments.

- Utilize training and information resources, which include:
  - National Institute of Standards and Technology (http://csrc.nist.gov/publications/PubsSPs.html)
  - FedRAMP (http://cloud.cio.gov/fedramp)
  - Information Systems Audit and Control Association (https://www.isaca.org/Pages/default.aspx)
  - International Council of E-Commerce Consultants (EC-Council) (http://www.eccouncil.org/)
  - Project Management Institute (http://www.pmi.org/en.aspx)
  - Cloud Security Alliance (https://cloudsecurityalliance.org/)