# (U) Intelligence Community Service Operations Group (IC SOG)

# STATEMENT OF WORK (SOW)

**15 December 2014**

## APPENDICES

## Statement of Work (SOW)

### 1.0 (U) Introduction/Background

(U//FOUO) The Intelligence Community Service Operations Group (IC SOG) Program delivers to the National Security Environment (NSE) interagency web-enabled information sharing and collaboration. The capabilities are comprised of search and content discovery, collaboration, media sharing, authentication and authorization, web-space services and applications. These capabilities known as Intelink services allow members of the IC to collaborate in a common shared space. The IC SOG ensures all services are secure, interoperable, and available to all IC stakeholders: Intelligence Community, National Defense, Homeland Security, Law Enforcement and Diplomatic/Foreign Relations. IC SOG operates and maintains these capabilities for over 275,000 users twenty four (24) hours a day, seven (7) days a week on the national intelligence enterprise comprising four fabrics - Top Secret, Secret, Unclassified and Top Secret/Coalition, accessed by members of the National Security Environment.

(U//FOUO) The IC SOG provides near real-time system monitoring of IC SOG systems and services and provides a service desk for all users to access technical support to resolve all issues and concerns. IC SOG identifies and deploys enhancement of current tools and services as well as new tools and services that address intelligence mission needs.

### 2.0 (U) Scope

(U//FOUO) The Contractor shall operate and maintain all operational centers for IC SOG Services. The Contractor shall manage the configuration of operating systems, applications and architectures and implement a process to accept and incorporate changes to the operational baseline to ensure the operational baseline is properly maintained. The Contractor shall provide security operations at the IC SOG and for Intelink Services, including activities related to physical, communications, information, and operations security. The Contractor shall maintain a standard hardware and software infrastructure, to include hardware standardization, standard build and implementation plans, operating systems, databases, and web and application servers. The contractor shall provide 24 hours, 7 days a week, 365 days a year operations and after-hours trouble resolution.

### 3.0 (U) Applicable Documents

- Intelink Configuration Management Policy and Procedures, effective 01 August 2011
- Intelligence Community Government Cloud Test Plan, version 26 September 2012
  - IC ITE Test Procedures
  - Test and Evaluations from GovCloud for IC ITE Established Procedures

- Inteldoc Standard Operating Procedures (SOP) For Service Desk, dated 04 April 2014
- IT Equipment Baseline, DPAS May 2014
- IC GovCloud Virtual Machine Systems established by IC ITE for GovCloud, 03 March 2014
- IC ITE Conceptual Architecture, draft 02 May 2013
- IC ITE Systems Engineering Processes (SEP), draft dated 27 January 2014, which includes:
    - System Development and Test Configuration Baseline

## 4.0 (U) Requirements

The Contractor shall provide Program and Project management for the following Intelink service lines: Service Operations and Maintenance, Service Desk, Identity and Access Management, Services Migration, and Operational Security and Information Assurance.

The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to -

(1) Furnish phase-in training; and

(2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

### 4.1 (U) Tasks

### 4.1.1 (U) Program Management, further noted in TTO-01:

(U//FOUO) The Contractor shall provide program oversight to ensure the effective execution of the IC SOG contract to include:

4.1.1.1. Designate one person as contract lead to act as the primary interface between the Contractor and the Contracting Officer's Representative (COR). This contract lead shall:

- Plan, resource, manage and execute each TTO
- Meet personnel staffing level requirements
- Confirm all contract deliverables (CDRLs) are delivered as required

4.1.1.2. Maintain the IC SOG Master Schedule.

- Track and update program accomplishments on the baseline Master Schedule and report findings to the Government PM Identify and track high-visibility delivery dates and cross-project dependencies and report findings to the Government PM

4.1.1.3. Provide a risk management plan and process to continually assess risk throughout the daily operations, implementation, update and release of new Intelink capabilities and services.

- Maintain a risk matrix identifying high and low impacts
- Recommend mitigation strategies to identified risks, and implement the strategies selected by the Government
- Update Government PM on current risks and associated mitigation strategies

4.1.1.4. Baseline and maintain a configuration management process to maintain Intelink system hardware and software baselines.

- Leverage the existing IC SOG Configuration Management Plan
- Maintain baselines for IC SOG systems' and services' IT equipment, software and licenses, and development and test environments
- Maintain and update the Intelink requirements repository

4.1.1.5. Provide document control services to administer, update and maintain the program's document repositories and web sites.

- Provide IC SOG document repository access control
- Maintain the IC SOG document repository organizational structure
- Ensure program information posted in the repository or web portal is current (Development, Test, meeting, and briefing documents)

4.1.1.6. Follow Quality Assurance (QA) processes for the delivery and maintenance of all capabilities and services.

- Designate one person as contract QA lead (must be independent from the development and test teams)
- QA lead shall review plans and procedures for accuracy and completeness
- QA lead shall maintain a Discrepancy Log and bring to management attention any outstanding discrepancy

4.1.1.7.  Provide property accountability oversight for all inventory, including:

- All Sensitive Compartmented Information Facility (SCIF) furnishings
- All office IT equipment
- All Intelink IT equipment
- All maintenance & special IT equipment

4.1.1.8. Provide SCIF access security control and maintenance services for two buildings at NSAW and their associated furnishings and mechanical services.

- Twenty four (24) hours a day, seven (7) days a week physically monitor SCIF main entrance access (manning the door during normal business hours M-F, by cameras on weekends and after-hours)
- Monitor all other SCIF access through electronic surveillance means
- Maintain a visitor log
- Provide escorts for non-cleared SCIF maintenance personnel

4.1.1.9. Provide IT Technical services to maintain the program’s SCIF office equipment and IT equipment.

- Oversee the repair or installation of IC SOG office equipment such as desktop computers, printers, phones, and fax as needed

### 4.1.2 (U) Service Operations and Maintenance, further noted in TTO-02:

4.1.2.1. The Contractor shall provide maintenance for all software applications and services available on all security fabrics across the five IC stakeholders: Intelligence Community, National Defense, Homeland Security, Law

Enforcement and Diplomatic/Foreign Relations. The Contractor shall provide the following Operations and Maintenance services:

- Operate and maintain IC SOG services in the existing service model, and support the evolution to new service models
- Monitor and track usage of services and systems for vulnerabilities, usage, and security
- Update Standard Operating Procedures (SOPs) and technical manuals
- Provide periodic software license inventory and usage reports
- Maintain office desktop and office automation services, system administration services, access control services, and software security updates
- Deploy software version upgrades, security patches and product updates
- Communicate schedule deployment of product and patch updates with effected users
- Collect metrics and metrics analysis for reporting

4.1.2.2. The Contractor shall maintain the Information Search and Discovery and associated services across the five IC stakeholders of the national security environment on all applicable fabrics. The Contractor shall:

- Work with organizations to optimize their websites for content search, discovery and delivery
- Operate and maintain search and discovery capabilities for content in Communities of Interest (COIs)
- Maintain access control to validate users only access content for which they are authorized (clearance, compartments, etc.)
- Maintain all service documentation, including user guides, technical operation and maintenance manuals, and assessment and authorization documentation
- Work collaboratively with other organizations to integrate their information services to ensure interoperability with IC SOG search services
- Operate and maintain these services in the existing service model, and facilitate the evolution to new service models
- Provide metrics and analysis regarding usage, trends, and user value

4.1.2.3. The Contractor shall maintain the Intelligence Community Applications Mall (Apps Mall) portfolio across the five IC stakeholders of the national security environment on all applicable fabrics. The Contractor shall:

- Perform product delivery, quality testing and maintenance releases

- Facilitate communication between software developers and IT professionals for operational system deployments
- Operate infrastructure across hardware and elastic software load balancing solutions in Government cloud and commercial cloud environments
- Collaborate with the Service Desk to diagnose and resolve Apps Mall user issues

### 4.1.3 (U) Service Desk, further noted in TTO-03:

(U//FOUO) The Contractor shall operate a Service Desk for IC SOG to provide twenty-four hour, seven day a week (24/7) system and service monitoring and respond to all user service requests across the five IC stakeholders: Intelligence Community, National Defense, Homeland Security, Law Enforcement and Diplomatic/Foreign Relations. The Contractor shall:

- Staff the Service Desk twenty four (24) hours a day, seven (7) days a week to respond to user requests
- Provide health and status monitoring for IC SOG and ICITE systems, networks, data flows, servers, applications, and services
- Provide Service Desk Tier 1 response to customer service requests (phone, email, fax, IM chat room, Intelink tickets)

### 4.1.4 (U) Identity and Access Management (IdAM), further noted in TTO-04:

(U//FOUO) The Contractor shall provide IdAM services which allow users and systems to access data for which they are cleared. The Contractor shall maintain the following IdAM services:

- IC Full Service Directory
- IC PKI Certificate Authority
- DoD PKI Local Registration Authority
- IC Digital Rights Management
- IC Login
- Common Services Attribute Service
- Common Services node of the Unified Attribute and Authorization Service (UAAS) federation
- Intelink-U Identity Federation
- Intelink Passport

The Contractor shall:

- Maintain up-to-date technology and integration to ensure ongoing service improvement
- Deploy updates to and patches of IdAM services

- Monitor, track and collect metrics on the usage of services for awareness of how the services are being used, by what service providers, what organizations, for what purposes, in what ways, with what technical standards, techniques, and results
- Generate and update SOPs and technical documents
- Conduct activities in compliance with applicable IC and federal standards

#### 4.1.5 (U) Services Migration, further noted in TTO-05:

(U//FOUO) The Contractor shall migrate IC SOG functions and services on the Top Secret, Top Secret/Coalition, Secret, and Unclassified fabrics from legacy to target environments.

(U//FOUO) The Contractor shall integrate services into Intelligence Community Information Technology Enterprise (IC ITE) components, and shall coordinate with these service providers to ensure the success of the transition:

- IC Cloud
- Enterprise Management Tools (EMT)
- Desktop Environment (DTE)
- Identification, Authentication, Authorization (IAA)

(U//FOUO) For IC Cloud, EMT, DTE, and IAA migrations, the Contractor shall:

- Follow procedures for the migration and convergence of IC SOG services
- Follow plans and collaborate on schedule for identified migrations
- Identify gaps in procedures/plans and update as applicable
- Perform all required testing and evaluations for migration
- Register services with appropriate security and authentication certificates according to standard regulatory procedures
- Verify data integrity and user access to IC SOG services and usability of the service within the environment
- Ensure all Government security and user authentication protocols are followed during migration
- Ensure legacy file path re-direct during migration
- Document all processes

#### 4.1.6 (U) Operational Security and Information Assurance, further noted in TTO-06:

(U//FOUO) The Contractor shall protect information and data from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction, and manage risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.

The Contractor shall:

- Maintain the protection, integrity, availability, authenticity, and confidentiality of data through the use of physical, technical and administrative controls
- Provide security engineering services to include risk management, awareness, and mitigation strategies and implement quality control mechanisms
- Manage the risk and security of IC SOG and Intelink computer systems and components connected the networks by complying with information security policies and procedures as established by the Government
- Sustain and monitor information technology security mechanisms and collaborate with Information Security organizations

### 4.2 (U) Deliverables or Data Requirements

(U) Data requirements and schedules are defined in the Contract Data Requirements List (CDRL), DD Form 1423.

### 4.3 (U) Facilities

(U) The effort shall be performed at either Government or Contractor sites or a combination of both.

(U//FOUO) For those tasks performed in Government facilities, the Government will provide on-site access to equipment customarily found in office spaces to include a telephone, desk, chair, storage cabinets, fax machine, copier, classified and unclassified computer systems, and classified storage facilities. Government facilities will be available for a maximum of 150 individuals at the Annapolis Junction site NBP304.

### 4.4 (U) Personnel

(U) The contractor shall provide a complete staffing plan at the time of contract award. The plan shall demonstrate how the contractor will be fully staffed in 45 days after contract award. The contractor shall maintain staffing levels during unexpected mission related requirements, emergencies, or surge requirements, as part of normal operational contingencies. All work hour requirements shall be coordinated with the appropriate CO and CORs.

(U) The contractor shall notify the CO and COR of any proposed personnel changes, as soon as the contractor is aware of such change and provide personnel replacements that meet the minimum personnel requirements of this SOW. The contractor shall provide a suitable replacement for staffing losses within 40 calendar days for non-key personnel. The contractor shall staff any key positions within 15 calendar days of notification of change. For key personnel the contractor shall provide appropriate data (e.g., professional résumés) to establish the credentials and suitability of key personnel under consideration for assignment to the contract.

(U) Below are the Key Personnel and the TTO to be supported:

| **Key Personnel LCAT** |
|---|
| Program Manager (PM) II |
| Comms/Network Engineer (CNE) II |
| Database Administrator (DBA) II |
| Help Desk (HD) I |
| Help Desk (HD) II |
| Help Desk (HD) III |
| Information Sys Security Engineer II |
| Information Sys Security Officer (ISSO) II |
| Project Manager I |
| Subject Matter Expert II |
| Subject Matter Expert III |
| System Administrator (SA) III |
| System Engineer (SE) I |
| System Engineer (SE) II |
| System Engineer (SE) III |

(U) The TTOs shall provide site-specific and position-specific duty hours and possible shift work.

(U) The contractor shall provide 24/7/365 on-call services.

(U) The contractor PM shall be the primary interface between the contractor and the Government COR.

(U) Any deviations from this policy require authorization from the CO.

## 4.5 (U) Security

(U) Unless approved by the COR, all Contractor personnel assigned to this contract must possess a current Intelligence Community TS/SI clearance for assignment to IC SOG Services IDIQ. The Contractor shall determine the initial minimum necessary employees with clearances needed to ensure a smooth uninterrupted transition between old and new contracts and with no interruption in IC SOG service.

(U//FOUO) The Contractor shall fully comply with all security requirements established for this contract by the DD254 (Contractor Security Classification

Specification). The contractor shall submit, update, and maintain a current Contractor Position Roster Log (CPRL), G5573. The CPRL is to be managed according to published guidelines from the Office of Security Services Policy Issuance 10-10, Industrial Security Program, dated March 1996. Additionally, the Government COR will provide Form G9006, Classification Guidance, for the appropriate classification guidance as needed. All contractor personnel requiring access to classified information systems or material shall possess a current TS/SI clearance with a full scope polygraph. A full scope polygraph includes both suitability and counterintelligence and is required for ongoing work with the Sponsoring Agency.

(U//FOUO) Contractor purchases of Information Technology (IT) (IT as defined by the Clinger-Cohen Act of 1996) and products of foreign origin (developed, manufactured, maintained or supported outside of the US or in the United States or its territories by an individual who is not a citizen of the United States or its territories) shall be subject to a Government risk assessment. The Government risk assessment will be performed prior to the Contractor purchasing items of this nature. The contractor may be required to implement risk mitigation countermeasures resulting from the Government's assessment. Any such countermeasures will be provided by the Contracting Officer (CO).

(U//FOUO) Contractor personnel shall comply with Operations Security (OPSEC) plans and policies provided by the Government. All subcontracts that require subcontractor employees to have access to classified information shall be subject to the same security concerns as set forth above.

(U//FOUO) In addition, there may be further security requirements levied upon personnel who are supporting compartmented efforts. A list of personnel who require additional security compartments shall be provided to and approved by the Contracting Officer (CO) and the Contracting Officer's Representative (COR) with a written justification, and will be notified by the COR upon security approval.

(U//FOUO) Upon the completion of the IDIQ or when an assignee no longer requires access to program information, that individual shall be immediately debriefed and all access controls (keycards, passwords, access tabs) shall be turned in to the SSO or appropriate Government office.

(U) The Government will provide access to relevant government organizations, information, and documentation, manuals, text briefs, and associated materials as required and available. Access shall be granted to classified networks as directed by the designated security authority.

(U//FOUO) In order to preserve the anonymity of the ultimate users of the materials and services of the IC SOG services, all purchasing, shipping, and receiving shall not be directly or indirectly associated with the Government. The

Contractor shall facilitate all communication with vendors and subcontractors so that the interest of the Government is not acknowledged.

(U) The Contractor shall comply with the following policy and directives when obtaining all hardware and software, to include open source software and freeware:

- NSA/CSS Policy 6-10, Control and Management of Licensed or Copyrighted Software

### 4.6 (U) Government Furnished Property

(U) There is no GFP for this contract.

### 4.7 (U) Travel

(U//FOUO) The Contractor shall be required to attend meetings, briefings, and perform other contract related tasks that require CONUS and OCONUS travel. Locations include Colorado, Texas and Virginia in addition to NSAW. All travel performed on this contract is subject to prior COR and/or CO approval.

### 4.8 (U) Training

(U) The Contractor shall provide personnel that are qualified to meet all requirements of the statement of work. Any training available at a commercial source shall be considered to be of general utility to the Contractor, and the training, labor and travel costs are not to be billed to the Government.

(U) Training will be provided by the government only when such software/systems are uniquely designed/fabricated by, or for, the Government and such training is otherwise unavailable to the Contractor. Courses conducted by Government schools may be made available to Contractor personnel where it has been clearly determined by the Contracting Officer (in writing) that training on specialized or unique government equipment is essential in carrying out the terms of the contract and the training is otherwise unavailable from a commercial source.

### 4.9 (U) Section 508 Compliance

(U) The Contractor shall conform to all Section 508 requirements when developing, procuring, or maintaining electronic and information technology products or systems.

**(U) APPENDICES:**

**(U) APPENDIX A – Service Line Descriptions B**
**(U) APPENDIX B – LABOR CATEGORY DESCRIPTIONS/QUALIFICATIONS**

# Appendix A – Service Line Descriptions B (Dec 2014)

**(U) Intelink Portfolio of Services – Critical & Non-Critical**

**(U) Blogs:** weblog service allowing contributors to add a new, or contribute to an existing, site established on a variety of mission topics.

**(U) Currency Converter:** a simple software code that is designed to convert one country currency into another in order to check its corresponding value.

**(U//FOUO) DNI-U network**: a private Sensitive But Unclassified network connecting the intelligence, defense, homeland security, law enforcement, and foreign affairs communities. Includes remote virtual private network connectivity to DNI-U.

**(U) eChirp:** the IC’s microblogging service, which provides situational awareness, alerts on breaking events, and additional communication methods for time dominant collaboration.

**(U) Gallery:** allows users to upload and manage photos, as well as share them with others in a central location. The service also features tagging to improve search and discovery.

**(U) Hosting Executive Agency Intelink Services:** Intelligence Community Services Operations Group (IC SOG) is managed by an executive agency within the IC. As part of its responsibility, IC SOG hosts the executive agency's site within the agency's own network until such time that the site is moved into the IC ITE.

**(U) IC Connect**: a real-time web-based presentation tool used to collaboratively create presentations, online training materials, and learning modules. It also facilitates web conferencing and user desktop sharing (Top Secret network only).

**(U) IC Digital Rights Management Services (ICDRMS):** allows originators to maintain dynamic control over the access and use of PDF documents, MS Office documents and HTML web content. When using ICDRMS to self-protect data, data managers retain dynamic control.

**(U) IC Prediction Market:** offers capability in a number of key IC functions, including coordination, real-time forecasting, hypothesis testing, and other still innovative functions for intelligence analysts and policymakers

**(U) Identity and Access Management (IdAM):** comprised of the following: Intelink Passport, IC PKI Certificate Authority, DoD PKI Local Registration Authority, IC Digital

Rights Management, IC Login, Common Services Attribute Service, Common Services node of the Unified Attribute and Authorization Service (UAAS) federation, and Intelink-U Identity Federation.

**(U) IntelDocs**: a web-based document management system providing document storage, simple document management, versioning, and access control. Users can share documents across agencies and commands and access their documents from anywhere with network access.

**(U) Intelink Button:** the Intelink Button is a JavaScript bookmarklet in your browser that allows authenticated Intelink users to perform a number of tasks such as creating a bookmark, create a chirp, shorten a URL, pin to IntelPin, and upload images to Gallery.

**(U) Intelink Home Page:** IC SOG maintains an Intelink Home page on all for networks providing a single point of access to all the tools and services for the users to experience. The home page provides the latest updates on national and international events affecting US and Allied interests as well as help on accessing and learning the Intelink applications and services.

**(U) Intelink Instant Messenger (IIM):** chat service for members of the IC, Department of Defense, Department of Homeland Security, and other agencies of the federal government. Users can maintain contact rosters (i.e., buddy lists), exchange private messages with other users, participate in conference rooms (group chats), and communicate in real time from their desktop.

**(U) Intelink Search & Discovery:** Intelink's primary search service, consisting of multiple components, that establishes and supports a comprehensive index of IC and stakeholder content and will return the pages most relevant to search terms.

**(U//FOUO) Intelink Service Desk:** operates 24 hours a day seven days a week year round and is highly critical component of the IC SOG program. It offers assistance and support to Intelink users and stakeholders to ensure proper response and resolution to all issues affecting Intelink customers and stakeholders. The Desk is comprised of three basic services: Customer Support, Systems and Service Monitoring, and Outage/Problem Triage. The Service Desk responds to inquiries regarding issues affecting the access and use of Intelink systems and services. The Service Desk monitors the health of all systems and services of the IC SOG to include networks.

**(U) Intellipedia**: the IC's collaborative wiki for intelligence and intelligence-related information where users can coordinate, communicate, and collaborate on issues and topics that affect the entire national intelligence enterprise.

**(U) IntelPin:** a virtual pinboard. IntelPin allows the user to organize and share all the content they are interested in from Intelink services. Users can browse boards created by other people to discover new things and find other users that share your interests. This allows them to gather related information from multiple Intelink Services and store them in a single, convenient location.

**(U) IntelShare:** web-based content management system allowing teams to collaborate on and publish documents, add web content, maintain task lists, implement workflows to automate and streamline business processes, and share information through the use of wikis and blogs.

**(U) iStory:** gathers content from Intelink services and other files to build Blogs, Word documents, and PDF documents. Search Intelink services to find media elements about the topic. Drag and drop text, photos or videos to bring together the media elements that will best illustrate a story. Reorder or delete elements in the story.

**(U) iVideo:** a video sharing application that allows users to view and share video content in a rich integrated environment. Users can easily share videos via this collaborative site that provides a forum for people to connect to and inform others across the IC.

**(U) Living Intelligence (LIS)**: a joint production system that helps increase IT efficiencies by reducing dependence on agency production systems to create approved content. This is a project between National Geospatial-Intelligence Agency (NGA) and Intelink aimed at transforming the vertical, agency-proprietary finished intelligence process. Living intelligence reduces duplication by moving the review process into the same place where transparent online collaboration takes place creating a joint "cloud" vetting system that brings transparency, more serendipity to the flow of information, broader peer review, and network effects to the official process not the informal process.

**(U//FOUO) Non-Attributable Internet Access Service**: disassociates users' web footprints from attribution to the U.S. Government (USG), enabling open source research and collection.

**(U) One-Way Transfer (OWT):** provides an enterprise-wide One-Way Transfer (low-to-high) capability for missions across the IC and partner communities. The current Enterprise OWT capability enables secure data transfer from the Unclassified fabric to TS/SCI, Secret to Top Secret/SCI, and Unclassified to Secret domains. OWT enables data sharing and services across security, organizational, mission, and business domains and be accessible to the entire IC community.

**(U) Remote Access/ Trusted Agent:** provides access to Intelink-U services through the Internet using DoD Common Access Card (CAC), similar federal Personal Identity Verification (PIV) tokens, and passwords, to authenticate to Intelink from the Internet.

**(U) RSS Reader**: referred to as an RSS aggregator is a tool for storing and managing RSS subscriptions. The user subscribes to a feed by entering the feed's link into the reader or by clicking an RSS icon in a browser that initiates the subscription process. The reader checks the user's subscribed feeds regularly for new content, downloading any updates that it finds.

**(U) Survey Tool:** used to collect information on a topic. Options allow the user to require the respondent to provide answers to any question type, change the order of the questions, and modify the question/answer after the survey has been created. Survey results can be reported in three formats: email, table, or Excel format. Individual survey results can be sent to a distribution list or viewed on screen during or after a survey is completed.

**(U) Tapioca:** social networking and collaboration environment that promotes unplanned collaboration between diverse employees.

**(U) URL Shortener:** takes a long URL and provides a shorter URL for distribution that will redirect the user to the original URL. This is useful when including links to pages in emails, where lines typically are broken at the 70–80 character mark. Also for presentations, instant messaging and chat channels, or anywhere else where line space is a valued commodity.

**(U) Web Analytics:** a state-of-the-art service offered by Intelink on all three fabrics. The service utilizes the Piwik Web Analytics package (http://piwik.org/ ) which is an open source analytics tool similar to Google Analytics. Utilizing this service, users will be able to track visitors to their site and gain valuable metrics. Metrics are provided in a customizable dashboard providing information such as number of visitors, return visitors, bounce rate, visitor browsers, visitor operating systems, and much more.

**(U) World Clock:** allows users to select multiple cities or locations and will display the current time in an analog or digital clock. If the user is logged in, the site will remember the selected clocks so they will appear the next time the user visits the page.

**(U)** Contractor shall support IC SOG office operations by providing the IC SOG office desktop and office automation services, with associated system administration services, access control services, and software security updates.

**(U)**

| **CRITICAL END-USER FACING INTELINK SERVICES (99.2% UPTIME)** | | | | | |
|---|---|---|---|---|---|
| **#** | **CRITICAL Intelink Services** | **NETWORKS** | | | |
| | | **TS** | **S** | **Unclass** | **Coalition** |
| 2 | Gallery | X | X | X | N/A |
| 3 | Hosting Executive Agency Intelink Services | X (FY15) | N/A | N/A | N/A |
| 4 | Identity Management (IdAM) | X | X | X | X |
| 5 | Inteldocs | X | X | X | N/A |

| | | | | | |
|---|---|---|---|---|---|
| 6 | Intelink Home Page | X | X | X | X |
| 7 | Intelink Instant Messenger | X | X | X | N/A |
| 8 | Intellipedia | X | X | X | X |
| 9 | iVideo | X | X | X | N/A |
| 11 | Maps ( Part of Search & Discovery) | X | X | X | N/A |
| 12 | Passport Attribute Service | X | X | X | X |
| 13 | Recent Intel | X | X | X | N/A |
| 14 | Search & Discovery | X | X | X | X |
| 15 | Service Desk Functions | X | X | X | X |

**(U)**

**(U)**

**NON-CRITICAL END-USER FACING INTELINK SERVICES (98% UPTIME)**

| **#** | **NON-Critical Intelink Service** | **NETWORK** | | | |
|---|---|---|---|---|---|
| | | **TS** | **S** | **Unclass** | **Coalition** |
| 1 | Blogs | X | X | X | N/A |
| 2 | Bookmarks | X | X | X | N/A |
| 3 | Currency Converter | X | X | X | N/A |
| 4 | Digital Rights Management | X | N/A | N/A | N/A |
| 5 | eChirp | X | X | X | N/A |
| 5 | IC CONNECT | X | N/A | N/A | N/A |
| 6 | IC Prediction Market | X | X | N/A | N/A |
| 7 | Intelink Button | X | X | X | N/A |
| 8 | IntelPin | X | X | X | N/A |
| 9 | IntelShare | X | X | X | N/A |
| 10 | iStory | X | X | X | N/A |
| 11 | Living Intelligence | X | N/A | N/A | N/A |
| 12 | Non-Attributable | N/A | N/A | X | N/A |
| 13 | One Way Transfer | X | X | X | N/A |
| 14 | Remote Access / Trusted Agent | N/A | N/A | X | N/A |
| 15 | RSS Reader | X | X | X | N/A |

| | | | | | |
|---|---|---|---|---|---|
| 16 | Survey Tool | X | X | X | N/A |
| 17 | Tapioca | X | N/A | N/A | N/A |
| 18 | URL Shortener | X | X | X | N/A |
| 19 | Web Analytics | X | X | X | N/A |
| 20 | World Clock | X | X | X | N/A |

**(U)**

### (U) Intelink Service Desk Operations & Customer Support

(U//FOUO)The Intelink Service Desk is currently comprised of 4 teams: Tier-1 Customer Support (aka "the Watch"), Tier-2 Customer Solutions, Accounts Team, and Training & Quality Assurance. While the entire Service Desk serves as administrators for most Intelink services, each team has unique roles and responsibilities.

(U) Tier-1 Customer Support Team

- (U) Continuously monitors the availability of all services and takes appropriate measures when a service outage occurs. This includes identifying which components of the service is down, accessing virtual machines, performing basic troubleshooting steps, restarting Linux servers, coordinating with service owners regarding escalations, and carefully documenting all service recovery steps related to an outage.
- (U) Serves as first point of contact Customer Service Representatives (CSRs) for customers contacting Intelink via multiple entry points, including phones, instant messages, emails, and tickets.
- (U) Provides technical assistance to customers for all Intelink Services.
- (U) Provides basic instructions on how to use Intelink services to external and internal customers.
- (U) Troubleshoots customer accounts and users' ability to log on to Intelink services.
- (U) Documents customer issues via tickets for the purpose of metrics gathering.

(U) Tier-2 Customer Solutions Team

- (U) Responds to all issues Tier-1 is unable to resolve which could involve investigation and in-depth collaboration with other internal/external teams and/or service owners.
- (U) Serve as subject matter experts for all Intelink services.
- (U) Provides Tier-1 phone coverage during trainings, meetings, emergencies, and shortages in personnel.
- (U) Assists Tier-1 resources with technical issues, application knowledge, and procedural instructions.
- (U) Receives and documents user requests for enhancement to Intelink services.
- (U) Represents the Service Desk and its customers in IC SOG meetings (i.e. ITEB, Requirements Review Board, IC ITE Operations Board).

- (U) Teams with Intelink service providers to provide in-depth testing and evaluation of new Intelink services and upgrades.
- (U) Provides communications to internal and external customers informed of changes to services, upgrades, outages, and current events deemed important to users.
- (U) Responsible for creating and updating FAQs and SOPs for Intelink services and IC ITE operations and services (i.e. GovPort, AppsMall), as well as the knowledge base of Intelink's ticketing system.

(U) Accounts Team

- (U) Processes emails and tickets from users requesting restricted Intelink accounts/services, which include Remote Access accounts, Non-Attributable Internet Service accounts, and Trusted Agent accounts.
- (U) Responsible for being subject matter experts for the aforementioned Intelink accounts/services and troubleshooting issues regarding the proper setup of these accounts.
- (U) Reaches out to organizations within the serviceable community to establish and maintain Trusted Agents as account administrators and informational points of contact.
- (U) Provides instructions to Trusted Agents on the use of restricted Intelink accounts/services and the correct protocols for administering accounts and assisting users of these accounts.
- (U) Regularly performs audits to ensure that users and Trusted Agents are compliant with the terms of service and guidelines for using their accounts.

(U) Training & Quality Assurance

- (U) Trains all new employees to the Intelink 24/7 Service Desk through a 3-week course to help new employees learn how to operate and maintain all of Intelink's services and applications as well as basic customer service techniques.
- (U) Prepares a variety of training aids and materials, and provides on the job training to all Service Desk technicians.
- (U) Collaborates with other Intelink teams for updates to current services and roll-out of new services to accomplish Service Desk training goals and objectives.
- (U) Assists Service Desk technicians with technical issues, application knowledge, and procedural policies as needed.
- (U) Performs regular quality assurance duties by reviewing communications to and from the customer as well as workplace performance of technicians to determine individual and group training needs.
- (U) Responsible for creating and updating FAQs and SOPs for Intelink services and IC ITE operations and services (i.e. GovPort, AppsMall), as well as the knowledge base of Intelink's ticketing system.
- (U) Serves as a first-line point of contact for any customer escalations.

**(U) Intelink Service Desk Technical Tier Strategy**

(U) Tier I/Level 1 (T1/L1) customer support is responsible for basic customer issues and minor technical problems. It is synonymous with first-line support, level 1 support, front-end support, support line 1, and various other headings denoting basic level technical support functions.

- (U) Tier I specialist gathers the customer's information and determines the customer's issue by analyzing the symptoms and determining the underlying problem.
- (U) The technician identifies what the customer is trying to accomplish so that time is not wasted on "attempting to solve a symptom instead of a problem." Once the situation is identified, the specialist can begin sorting through the possible solutions available.
- (U) Technical specialists in this group will handle straightforward and simple problems utilizing already established procedures, call trees and Intelink's knowledge management system to either resolve or escalate the issue. Personnel at this level have a basic understanding of the product or service but may not have the experience/knowledge required for solving complex issues.
- (U) Tier I operates out of a call center that operates extensive hours (24/7). When required, the technician will create incident reports in order to notify other business teams/units to satisfy user requests.
- (U) Tier I requires general knowledge of the products and or services provided along with terms and conditions offered by the business.

(U) Tier II/Level 2 (T2/L2) is more in-depth technical support than Tier I. Technicians assigned to Tier II are more experienced and knowledgeable on particular products and services. It is synonymous with level 2 support, support line 2, administrative level support, and various other headings denoting advanced technical troubleshooting and analysis methods.

- (U) Tier II technicians are responsible for assisting Tier I personnel in solving basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues.
- (U) It is important that the technician review the work order to see what has already been accomplished by the Tier I technician and how long the technician has been working with the particular customer. This is a key element in meeting both the customer and business needs as it allows the technician to prioritize the troubleshooting process and properly manage his or her time.
- (U) If a problem is new and/or Tier II technicians cannot determine a solution, they are responsible for raising this issue to the Tier III technical group.

(U) Tier III/Level 3 (T3/L3) is the highest level of service responsible for handling the most difficult or advanced problems. It is synonymous with level 3 support, back-end support, support line 3, high-end support, and various other headings denoting expert level troubleshooting and analysis methods.

- (U) Tier III individuals are considered experts in their fields and are responsible for assisting both Tier I and Tier II personnel, and for the research and development of solutions to new issues as well as Tier I and Tier II unresolved issues.

- (U) Tier III technicians have the same responsibility as Tier II technicians in reviewing the work order and assessing the time already spent with the customer so that work is prioritized and time management is sufficiently utilized. Technicians will work to solve the problem with the customer when it becomes apparent that Tier I and/or Tier II technicians were unable to discover a solution. In some instances, the product cannot be salvaged and must be replaced. Such extreme problems are also sent to the original Intelink service providers for in-depth analysis. If it is determined that a problem can be solved, Tier III is responsible for identifying one or more courses of action, evaluating each of these courses in a test case environment, identifying their pros and cons, and implementing the government's chosen solution to the problem while complying with the governance process. Contractor will be responsible for continuing troubleshooting and analysis as necessary.

(U) Tier/Level 4 (T4/L4) represents an escalation point beyond the organization. This is generally a hardware or software vendor. Within a corporate incident management system it is important to continue to track incidents even when they are being handled by a vendor and the Service Level Agreement (SLA) may have specific provision for this.

**(U) Intelligence Community Information Technology Enterprise (IC ITE)**

(U//FOUO) In 2011, the Director of National Intelligence (DNI), in conjunction with Intelligence Community (IC) leaders, approved an ambitious new and more efficient direction for planning, developing, and operating IC Information Technology. This direction, known as the Intelligence Community Information Technology Enterprise (IC ITE), paves the way for a fundamental shift to operation as an IC-level Enterprise.

(U//FOUO) IC ITE (pronounced "eye sight") is a transformative strategy to further the DNI's vision of intelligence integration by revolutionizing the IC Information Technology's operating model. IC ITE moves the community from an agency-centric IT architecture to a common cloud-based platform where technology, information, and resources can be easily and securely shared.

(U//FOUO) By managing and providing the community's IT infrastructure and services as a single enterprise, the IC will not only be more efficient, but will also establish a powerful platform to deliver more innovative and secure technology to desktops at all levels across the intelligence enterprise. These new capabilities, with seamless and secure access to community-wide information, will positively and deeply change how users communicate, collaborate, and perform their mission.

(U//FOUO) The National Security Agency's contributions to IC ITE include the IC Applications Mall, IC Government Cloud, and Identity, Authentication, and Authorization Service.

(U//FOUO) IC Applications Mall provides access to community and agency franchise stores where users can discover mission and business capabilities to foster communities and connections across organizational boundaries.
- (U//FOUO) IC Government Cloud (IC Cloud) in partnership with CIA's Commercial Cloud Service (C2S) (the "IC Cloud") provides on-demand data analytic, storage, and application hosting services for the Intelligence Community. The community can use the Government Cloud to securely share their data and information with other IC agencies, providing an opportunity to bring together, under a common secure framework, historically disparate IC datasets and apply "Big Data" analytics against those datasets in order to discover unknowns, correlate IC-wide target identifiers, and more. The IC Cloud eliminates the need to move data between agencies, significantly reducing data duplication.

**(U) IC Apps Mall**

(U//FOUO) The Intelligence Community Applications Mall (IC AML), also called Apps Mall, is a common virtual environment where authorized users can discover and use applications pertinent to their mission or business needs. Similar to a physical mall, the IC AML provides a place where producers and consumers can interact easily, securely, and more collaboratively.

(U//FOUO) The Apps Mall is hosted for the community by the Intelligence Community Services Operations Group (IC SOG) IC Service Operations on the Top Secret network. It is a web-based software environment which enables users to obtain and utilize applications (a.k.a. "widgets") that have been made available to the IC. Developers from agencies within the IC will produce widgets and share them with users of other agencies via Apps Mall.

(U//FOUO) The Apps Mall operates on a software platform known as Ozone Widget Framework. The framework allows users to access, visually organize, operate, and integrate multiple applications from across the enterprise for the discovery, analysis, and creation of data. Utilizing standards, component libraries, templates, and following a governance process that fosters collaboration and reuse, the Apps Mall makes available uniform widgets developed by other agencies throughout the community for mission needs.

(U//FOUO) These widgets are web-based applications that can easily be added to websites, blogs, or other specialized pages in order to provide specific functionality enhancements through executing small amounts of software code. The Apps Mall has widgets include visualization, mapping, tagging, query, data analysis, search, content hosting, collaboration and others much like those that exist in the consumer environment. Some tools are enhanced with the capabilities to interact with others widgets and the growing IC components of Apps Mall. Users can get the most up to date listings of available widgets by accessing the Community Store within IC Apps Mall. IC elements also operate stores containing their own applications.

(U//FOUO) The IC Apps Mall is PKI enabled and uses IC PKI credentials in the GovPort service. The user identity from the presented IC PKI certificate contains the user organization among other attributes for authorization.

(U) Users can rate and provide feedback as well for the benefit of others. Users can preview the widget to try it out and see if it is something that might be useful to them.

(U//FOUO) The IC Applications Mall consists of production and staging instances of the IC AML Webtop and IC AML Community Store on JWICS. There is a community staging area on the Unclassified network available as well.

(U//FOUO) Developers with widgets to deploy should do so in the staging instance first to test the widget(s) (functionality, interoperability, and access issues) before registering the widgets in the production Community Store. An initial governance process for how the widgets are approved has been identified by the IC Joint Engineering Teams (JET). Every widget must provide and maintain the IC widget entrance criteria.

(U//FOUO) The current release has IC widgets submitted by the IC Service Operations Group (IC SOG) and other agencies. The Community Store continues to expand with additional widgets both from across the IC Community as they become available and meet the entrance criteria.

(U) A new store model is currently being implemented, to provide a Software-as-a-Service-based store capability for IC elements' use, vs. their maintaining their own store infrastructures.

(U//FOUO) The AML Website uses Ozone Widget Framework (OWF) and the Community Store uses Ozone Marketplace for all instances on the Top Secret and Unclassified networks.

**(U) IC Desktop Environment**

(U//FOUO) Another IC ITE component is the IC Desktop Environment (DTE), being delivered jointly by DIA and NGA.   A description is below.  DTE is relevant to IC SOG contracts for two reasons.

- (U//FOUO) Because DTE will be the common office automation desktop for IC personnel, the IC SOG expects to migrate to DTE services from its current locally-provided desktop services on the Top Secret fabric.
- (U//FOUO) Some IC SOG user-facing services may be migrated to DTE in some fashion.

(U//FOUO) The **IC Desktop Environment (IC DTE)** is an IC ITE initiative to create and manage a common computer operating system and associated business services, improving collaboration and enhancing mission performance. It leverages existing technologies to make business services available at any IC location, and at all three security levels. IC DTE provides a secure, thin-client desktop infrastructure for IC users using virtual desktop capabilities that include office automation, secure phones, video teleconferencing, instant messaging, and application-sharing enabled by an IC common Active Directory. Future implementation phases will expand TS/SCI/NOFORN user access to include higher Community of Interest (COI) access control levels for security of data and user accessibility extended into 5-Eyes and TS/Coalition collateral domains. IC DTE will provide IC users a single set of login credentials to access e-mail, information-sharing databases, desktop video teleconference capabilities, as well as select mission applications, from any desktop in the IC.

(U//FOUO) ***IC DTE business services include:***

- (U) A common, standardized desktop operating system for both thick and thin clients operating at the TS/SCI/NOFORN classification level. Initial desktop operations will only involve the Microsoft operating system and thin clients
- (U) Access to a virtual desktop from the user's current legacy endpoint configuration
- (U) A common directory service for user authentication, authorization, and Attribute-Based Access Control (ABAC).
- (U) Account management, including an IC Common Desktop user Active Directory, email, and home directory.
- (U) File collaboration and sharing (i.e., SharePoint)
- (U) Office automation capability (i.e., email; print services; and document, spreadsheet, and presentation creation and editing tools).
- (U) Unified Communications (i.e., secure soft phone and video conferencing, instant messaging, presence awareness, shared applications and whiteboards, and services integrated into room-based Video Teleconference (VTC) infrastructures.
- (U) Streaming video to include Video-on-Demand (VoD), including multi-cast.
- (U) A service catalog with all approved desktop hardware and software lists to enable IC DTE services.