Data Handling and Protection of Need-to-Know Data in a Need-to-Share Net-centric Enterprise

Jeffrey B. Skelton
The MITRE Corporation

CONFERENCE PAPER

The execution of multiple programs pursuing technologies to enable the Department of Defense (DoD) vision for network-centric (net-centric) Space Situational Awareness (SSA) capabilities has revealed a gap in existing data protection and handling requirements and policies. This paper presents the findings of an assessment of existing policies and classification guidance along with proposed actions applicable to the net-centric SSA Enterprise. The proposed actions are intended to support the migration to a net-centric SSA Enterprise while ensuring data access and handling protections are in place until such time as policy and guidance updates can be aligned, approved and released.

1. SSA ENTERPRISE VISION

The Department of Defense (DoD) and its supporting organizations share a common goal of delivering cross-mission information superiority through developing Enterprise-level data and information sharing between data producers, data processing nodes and both anticipated and unanticipated consumers. Key to achieving the net-centric Enterprise-enabled capabilities is opening mission-oriented closed networks and making data visible, accessible, understandable, trusted and interoperable to all users.

For the Space Situational Awareness (SSA) Enterprise, this vision entails enabling sensors and Command-and-Control (C2) nodes to expose and distribute data of value for discovery and use by currently known and future users. As the participating systems within the SSA Enterprise will consist of newly acquired, net-ready systems as well as existing non-enabled legacy systems, achievement of the envisioned Enterprise will evolve over time with several stable but intermediate forms.

2. SSA DATA TYPES

As defined in the SSA Initial Capabilities Document (ICD), SSA can be generally decomposed into four functional areas. These functions are defined as [1]:

- **Detect / Track / Identification (D/T/ID):** The ability to search, discover, track and maintain custody of space objects and events, distinguish between objects and to recognize objects as belonging to certain types, missions, etc.
- **Threat Warning / Assessment (TW/A):** The ability to predict and differentiate between potential or actual attacks, space weather environment effects, and space system anomalies, as well as provide timely status of friendly forces.
- **Characterization (CH):** The ability to determine strategy, tactics, intent and activity, including characteristics and operating parameters of all segments (ground, link, and space) of space systems, particularly foreign and adversary, and threats posed by those systems.
- **Data Integration and Exploitation (DI&E):** The ability to correlate and integrate multi-source data into a single common operating picture (COP) and enable dynamic decision making through SSA services. This capability enhances the other three capability areas of SSA (D/T/ID, Threat Warning and Assessment (TW&A), and CH) and provides the ability to identify, correlate and integrate multiple sources of data and information and to provide SSA services.

Generally, the identified SSA sensor data for exposure can be grouped into D/T/ID, CH, and Sensor Command and Control (C2) categories. The groupings below are representative of the data elements within each category but are not intended to be complete. With many different types of data producers and evolving mission needs it is anticipated that additional data types, such as space weather, may be defined as the SSA Enterprise matures.

SSA related Data Types:

- D/T/ID: Metric Observations, Element Sets, State Vectors with/without Covariance, Pointing Angles (optical).
- CH: Space Object Identification (SOI) [all forms], Radar Cross Section (RCS) [all forms], Signal to Noise Ratio (SNR) [all forms], Visual Magnitude, Calibration Data.
- Sensor C2: Tasking, Tasking Status Information, Mission Plan Data, Radar Scheduling Data.

While specific classification guidelines exist for each specific sensor type generating the Positional and Characterization data types identified above, general guidelines to be considered regarding classification and release of sensor generated data include:

- Generally, data assumes the classification of the object observed [2].
  - Data collected on satellites with UNCLASSIFIED Element Sets is UNCLASSIFIED
  - Data collected on satellites with SECRET Element Sets is classified SECRET
  - Signature data (e.g. Visual Magnitude Imagery, SOI) taken on deep space Uncorrelated Targets (UCTs) is classified SECRET and becomes UNCLASSIFIED if UCT data is correlated to an unclassified known object [2].
  - Signature data collection on certain objects is prohibited.
- Signature/Characterization data carries additional classification guidance [3].
  - Signature data assumes the classification of the object observed. Data release requires approval of United States Strategic Command (USSTRATCOM)/J3 or Joint Functional Component Command for Space (JFCC-SPACE)/J95.
  - Aggregation of Signature data (i.e., a database of data) assumes the classification of the object observed. Data release requires approval of USSTRATCOM/J3 or JFCC-SPACE/J95.

Additional data types and products are likely to be available net-centrically from C2 and other processing nodes. These additional data types may fit into one of the categories listed above or may require identification of additional categories and controls.

3. UNDERSTANDING ARCHITECTURES

In order to present and understand the issues between the 'need-to-know' and 'need-to-share' paradigms, an understanding of the underlying architectural forms is needed. Fig. 1 presents a simplified, high-level connection diagram of the current space surveillance network of sensors, consisting of dedicated and contributing radar and optical sensors located across the globe. Sensors are tasked by the Space C2 node and report collected observations and metric data over dedicated point-to-point communications links to C2 and other forward users. The C2 node is also the release authorization point for making data and information products available to authorized users

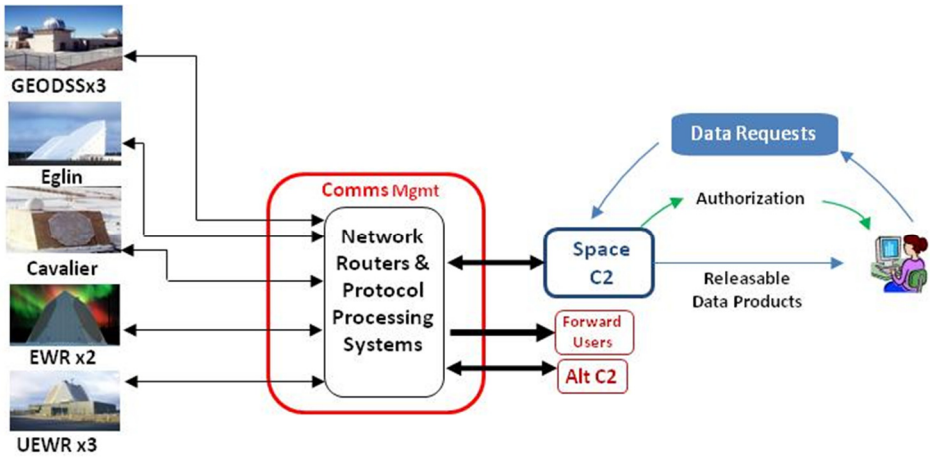

Fig. 1. High-level connectivity diagram of current Space Surveillance Network (SSN)

The processes and policies regarding data handling and access that govern today's architecture are documented and established, and provide mission assurance while accommodating limited and controlled data sharing. Not all data collected or produced by participating sensors is communicated to C2 and forward users, but only that data critical to the accomplishment of the space C2 and forward user missions, largely due to limited bandwidth of existing communications.

Legacy space surveillance systems are planned to be net-enabled to make data available via the Global Information Grid (GIG) over the next several years. While participating systems are transitioned to net-centric operations, it is envisioned that stable, intermediate forms of the SSA Enterprise will co-exist in parallel with the legacy communications network, as presented in Fig. 2 below.

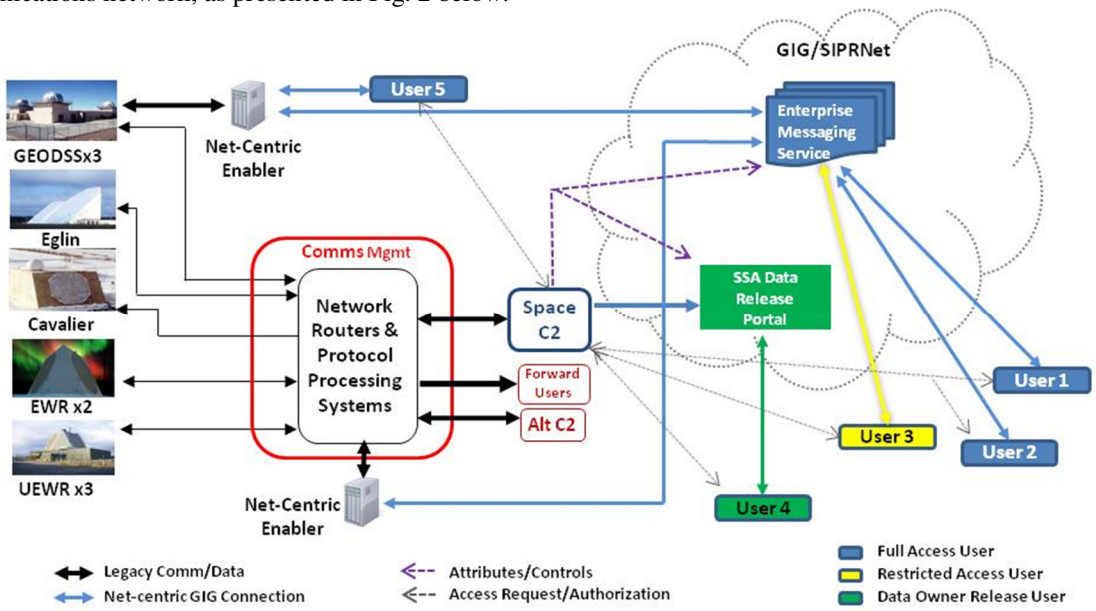

Fig. 2. Anticipated intermediate form of SSA Enterprise

Reflecting the goals and Net-Ready Key Performance Parameters (NR-KPPs) defined in Chairman Joint Chiefs of Staff Instruction (CJCSI) 6212.01E, the vision of the net-centric SSA Enterprise facilitates the exposure of many more SSA related data types to a broader range of authorized users connected to the GIG. Fig. 2 includes the connectivity and exchanges shown in Fig. 1 for today's existing SSN, but also depicts the planned deployment and operations of net-centric enabling systems at sensors (e.g. GEODSS sidecar) and primary communication node locations. These net-centric enablers are adjunct systems that on a non-interference basis facilitate the single/bi-directional flow of eXtensible Markup Language (XML) formatted data and message exchanges with anticipated consumers.

In the SSA Enterprise paradigm, data sources make identified data types available to *authorized* GIG users via net-centric services. It is planned that most users receive data from sources via Enterprise Messaging Service topics hosted and managed by Defense Information Systems Agency (DISA). In addition, use of other DISA-provided core services such as user authentication is planned for the SSA Enterprise. Light-colored arrows in Fig. 2 reflect the access request/authorization exchanges between consumers and the data owner(s). Different color users depict different access authorization permissions granted to consumers with varying qualifications.

In most cases the net-centrically exposed data set contains additional data types not currently transmitted to forward users over the existing point-to-point communications circuits. In the near-term, legacy point-to-point communications paths used for official mission execution (e.g. Space Control, Missile Warning) will remain in place to ensure mission assurance, reliability, and survivability requirements can be maintained. New users (or consumers) and evolving mission capabilities will be able to leverage the exposed data sets to support emerging warfighting capabilities.

4. SSA DATA SHARING PARADIGM

The data available for sharing in today's SSN as shown in Fig. 1 is limited to the data currently communicated from supporting sensors to the C2 node. It is possible using existing processes to request and receive, but not in real-time, sensor-held data elements within certain time constraints. As illustrated in Fig. 1, sharing 'points' on the closed network of the 'as-is' SSA network generally facilitates two tiers of data sharing: notionally Tier 1 *Official* Mission Users and Tier 2 *Other* Mission Users. Tier 1 users are those represented in the connectivity diagram directly connected by the point-to-point connections to the sensors and C2 nodes. These users comprise the processors and analysts who consume sensor data to produce data products to support the space control mission areas.

Tier 2 users would comprise the rest of the consumers of space data and products processed and assessed for releasability to authorized users or entities. Requests for space data and products is managed by the C2 node using their established "Interim Commercial and Foreign Entities (CFE) Data/Analysis Redistribution Approval Process", also referred to as the Form-1 process. This process can be considered to reflect the fact that the sensors depicted in Figs. 1 and 2, are not classification and release authorities, but are bound by existing security classification guidance and policies established by the respective data owner(s). Tier 2 users may or may not include other military, government, or civilian organizations, research organizations, commercial entities, or even amateur space enthusiasts. Tier 2 users can be supported by unclassified (uncontrolled and controlled) or classified data products, as determined by their unique qualifications and needs. Procedures are in place for authorizing and controlling data release to foreign entities as well as for general public release approvals.

The idealized image of the SSA Enterprise data sharing model most often described presents an Enterprise where mission barriers are lowered and information is shared freely amongst and across agencies, organizations and entities. The intent is to break-down stovepipe systems and networks in order to achieve broad levels of interoperability and to accommodate future, unknown capabilities enabled by information superiority. The intermediate SSA Enterprise form depicted in Fig. 2 implies evolution in the desired direction. The most immediate challenges with the SSA Enterprise appear to be focused on achieving the required mission assurance, survivability, reliability and timeliness within the Enterprise to eventually retire the legacy networks. Exposing data is relatively straightforward; achieving an operationally suitable and effective capability is the challenge.

5. ISSUES

To facilitate cross organizational, cross-program integration topics across the SSA Enterprise, the Mission Integration Forum (MIF) was established as a joint endeavor between Electronic Systems Center (ESC), Space and Missile Systems Center (SMC), and Air Force Space Command (HQ AFSPC), along with regular participation from other organizations such as USSTRATCOM, DISA, and others. In mid-2011, concerns were raised at the MIF about how multiple, independent programs pursuing net-centric data exposure and consumption capabilities would address data handling, access control, and authorization. An Integrated Product Team (IPT) was stood up to bring together technologists, operators, command leads and data owners to identify requirements needs, gaps and disconnects within governing policies related to data security. While several specific requirements were identified against existing programs and certain data types, at the heart of the issues were concerns about achieving balance between the Enterprise-vision of 'Need-to-Share' while retaining appropriate protections for 'Need-to-Know' constraints.

As described in the November 5, 2010 AFSPC Data Integration Memorandum, "the vision for AFSPC net-centric sensor operations is an interoperable, capability-focused suite of sensors, associated applications and services to deliver effects to warfighters and other users across the DoD, Intelligence Community, civil, commercial and foreign entities." The DoD net-centric data strategy has been refined to establish a well-documented and commonly understood top-level requirement that can be summarized as:

> *Data assets, services and applications on the GIG shall be visible, accessible, understandable, and trusted to authorized (including unanticipated) users* [4].
>
> ***By definition: Authorized User:*** *Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function* [4].

For the sensors producing data in support of SSA, many policies, instructions and guidance documents are currently applicable and in force. Some systems supporting multiple missions including space surveillance, missile warning and missile defense carry mission specific classification guides with which they must comply. Reviews of applicable and updated DoD Instructions, United States Strategic Command (USSTRATCOM) polices and US Air Force manuals and guidance documents are currently underway and Table 1 presents a partial list of reviewed documents containing requirements and references reflecting 'need-to-know' and access authorization controls. Several of the reviewed documents cite as the fundamental requirements for access to classified information as: A mission-based need-to-know, an appropriate security clearance level, and a signed Non-disclosure agreement.

Table 1. Guidance and Policies citing 'Need to Know' requirements.

Document Title	Signature Date
DoD Manual 5200.01 Vols 1 & 3	24 Feb 2012
DoD Instruction 8320.02	15 May 2012
Executive Order 13526	29 Dec 2009
Ballistic Missile Defense System (BMDS) Security Classification Guide (SCG)	19 Oct 2010
Dedicated Space Surveillance Sensors Security Classification Guide (SCG)	30 Sept 2005
Air Force Instruction 31-401	1 Nov 2005
AFSPC Data Integration Memorandum	5 Nov 2010

Current processes for authorizing user access requests to data and information sources are not directly transportable to the SSA Enterprise. Existing policies and processes are in place for manual management of data and authorized users but in the context of the SSA Enterprise, adapting manual processes to the number of projected human-to-machine and persistent machine-to-machine sharing interconnects becomes unwieldy. Process and policy owners will quickly have to define and publicize new mechanisms as the operational SSA Enterprise begins to emerge in years beyond 2012.

6. WAY AHEAD

The SSA Data Handling IPT findings largely restated requirements for programs to comply with existing policies and classification guidance for granting users access to exposed data. In spite of the manual level of effort required, it was proposed that existing processes used to manage and authorize data access controls be modified and leveraged until a suitable replacement process is defined and implemented. In order to support the broad sharing of SSA data envisioned for the Enterprise, the IPT also proposed that data owners define and allocate requestor attributes to data types to facilitate granular, tailored access controls for anticipated requestor types.

In the months following the submission of the IPT findings, significant activity by organizations including DISA and AFSPC have begun to close the identified gaps to achieving the secured data sharing of the Enterprise. With the latest release of Enterprise Messaging service, DISA has implemented the necessary attribute based controls to enable data owner management of access to messaging topics. This capability provides data owners a significant improvement in access controls over the previous binary (e.g. Yes/No) access options.

Similarly, AFSPC/A5C has taken lead on engaging with stakeholders to bring closure to open issues related to organizational responsibilities, needed procedures and processes, and socializing operational scenarios and sequences for Enterprise events. Closing the gaps in these areas will significantly benefit the achievement of the SSA Enterprise, and enable alignment of governing policies and instructions regarding data sharing. Perhaps most importantly, closing the gaps in requirements and processes should increase coherency in data sharing and protection implementations across programs supporting the Enterprise.

At the present time, there remain two primary issues to be addressed by the community, data owners and SSA Enterprise leadership. First, new data types are planned to be exposed consisting of data generated by producers that is not currently shared. Stakeholders need to review data exposure elements that are not transmitted from data producers currently with particular attention to compliance with governing classification guides and to resolve any

potential data aggregation risks. As new data types are identified for exposure, classification guides may require updates to appropriately protect data items.

Second, in parallel with the development of new, adaptable authorization and access management processes, it was also concluded that broad information sharing capability implies a broad selection of attributes that can be used to control at a granular level which data users can or cannot access. As depicted in Fig. 2, SSA data is accessible at multiple points across the Enterprise to authorized users depending on their needs and assessed access attributes identified by the data owner(s). Requestor attributes as defined by the data owner can determine where data is accessed along the SSA processing flow. Data access may be granted directly from sources/sensors, from the C2 node, or post data owner release determination based upon requestor need to know and where data is accessed along its processing chain. As the access control attributes evolve and mature, the resultant number and content of required messaging topics can be implemented to align data exposure with requestor attributes to achieve sharing as broadly as possible.

7. REFERENCES

1. Space Situational Awareness Initial Capabilities Document (SSA ICD),January 2012
2. Dedicated SSN Sensors Security Classification Guide, 30 September 2005
3. Space Surveillance Operations Security Classification Guide, 1 July 2007
4. Department of Defense (DoD) Information Enterprise Architecture (IEA) Version 1.2, May 2010