



Interconnect Security Agreement (ISA)

Between

Company A

And The

Aviation Systems Division

**Aviation Systems Division
National Business Center
U. S. Department of the Interior**

**Property of the United States Government
This Document Contains Sensitive But Unclassified
Information**

Do not remove this notice
Properly destroy when no longer needed

1. Overview

For clarification, the following definitions are offered:

- Company A Network provides aircraft tracking data.
- Aviation Systems Division (ASD) manages the Interagency Aviation Systems Local Area Network (IAS-LAN) that COMPANY A will need access to send aircraft tracking data.
- Automated Flight Following (AFF) is the application hosted within the ASD Data Center and will receive the aircraft tracking data from COMPANY A.
- SolutionPro, Inc. (SPRO), Boise, ID manages the data center and is the hosting provider for the IAS-LAN.

COMPANY A and ASD agree to connect their networks for the purpose of providing AFF system users access to Aircraft Tracking data provided by COMPANY A. The approach outlined in this agreement is intended to provide AFF with a network solution that provides capabilities designed to maximize the availability and reliability of applications services to COMPANY A. The interconnection agreement includes:

- One primary network connection to ASD Data Center in Boise.
- An additional network connection into AFF Disaster Recovery Network Access Point.
- A backup connectivity method for use in the event of the loss of primary connectivity.

All connectivity entering COMPANY A's network will possess a source Internet Protocol (IP) (TCP/IP) address range that is an American Registry of Internet Numbers (ARIN) registered address.

Connectivity entering ASD's network will pass through several layers of network and server-based controls including Intrusion Detection Systems (IDS), packet filtering systems, and proxy filtering systems, as appropriate.

Additionally, all traffic that originated from the Internet (outside COMPANY A's internal network) is not permitted to the ASD network unless the customer has previously:

- Encrypted from desktop to Customer perimeter using strong encryption methods (128 bit, SSL).
- Authenticated the connection using strong (eight characters with mixed case, numbers, and special characters) passwords.

2. Proposed Level and Method of Interconnect

Figure 1 illustrates the proposed network connectivity package for delivery of aircraft tracking and messaging data. The connectivity package includes the following three types of connectivity.

- Primary Connectivity
- Back-up Connectivity
- Disaster Recovery Connectivity (including disaster recovery testing)

The specific technologies used to interconnect the customers network and the ASD network is dependent on the three following primary factors:

- The number of COMPANY A processing sites to which AFF requires access.
- The number of servers requiring access to applications (this includes the concurrent user and the total number of users).
- The specific services upon which the applications are based. For example, WWW.

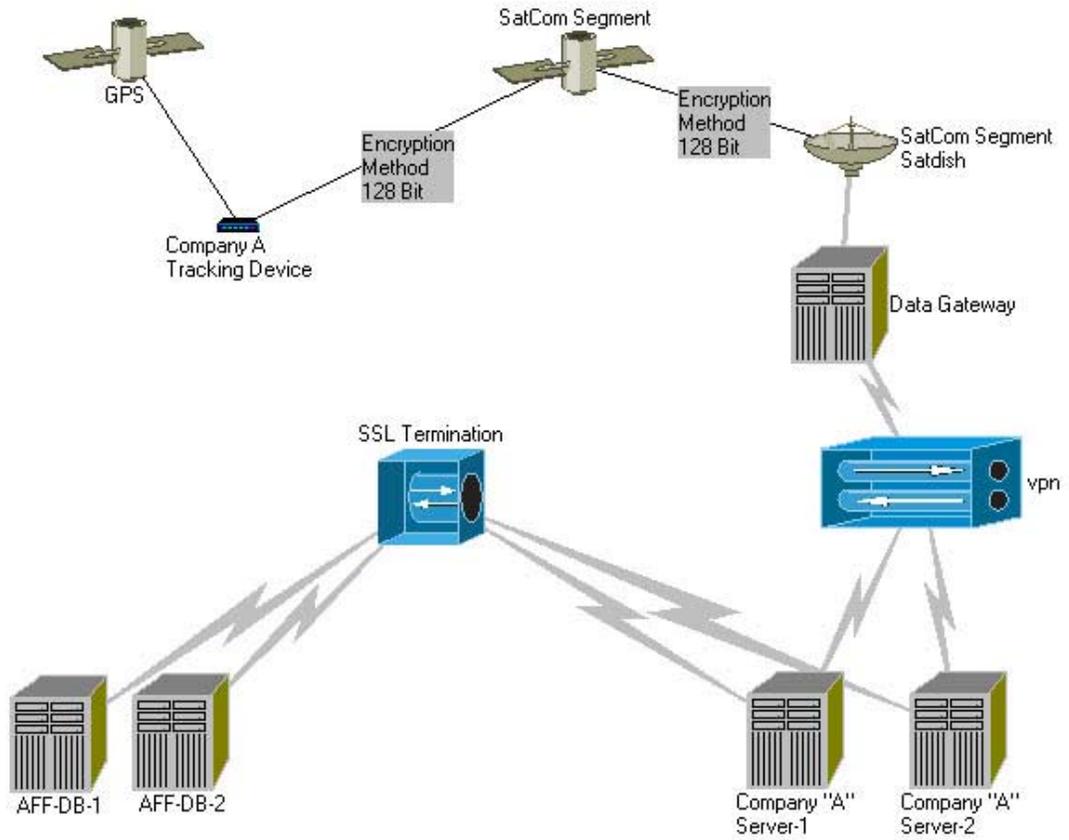
Connectivity between COMPANY A's application production environment and the AFF internal application production environment shall be allowed. COMPANY A will not allow internal AFF or ASD desktops to access COMPANY A's organizations networks. AFF will not allow internal AFF desktops to access COMPANY A's organizations networks. ASD will not allow internal ASD desktops to access COMPANY A's organizations networks. Additionally, a COMPANY A's internal network will not be permitted to access AFF internal desktops or to access to other customer networks.

AFF supports the following Network protocols:

- HyperText Transport Protocol (Secure), (HTTPS)

HTTPS is the recommended method for primary connectivity to the COMPANY A. The inherent capabilities of the technology make this service offering both cost-effective and scalable to meet future growth requirements.

Figure 1: — High Level Diagram of COMPANY A / AFF Connectivity Primary Connectivity — AFF and COMPANY A will use HTTPS a primary data transfer protocol.



**Property of the United States Government
This Document Contains Sensitive But Unclassified
Information**

Do not remove this notice
Properly destroy when no longer needed

3. Impact on Existing Infrastructure and Operations

There is no impact on ASD's existing infrastructure and operations as a result of this network interconnection. The network was designed to support multiple connections of this type.

4. Hardware

No new hardware is required at ASD Data Center to support this connectivity.

5. Software

The Cisco IOS levels will be maintained and kept current (current maintained production release as defined by the hardware vendor.) Patches will be applied for the IOS for the hardware, as vulnerabilities and "fixes" are made available and commensurate with the risk associated with the vulnerability. Access Control Lists (ACL's), the Firewall Feature Set, and other security controls will be fully implemented before production traffic is allowed to traverse the connection and as customer requirements and risks dictate.

Note: ASD will not allow traffic from other IAS-LAN customers to be routed through this network and into another AFF customer's network.

6. Roles and Responsibilities

ASD and SPRO technical staffs will manage the network interconnection between the Internet and the IAS-LAN up to the point of demarcation which is SPRO's perimeter connection to the Internet. The point for the primary connectivity is the COMPANY A Data Center. The specifics of this agreement are delineated below.

Network Management — Management of the interconnection between the two organizations is performed from the two following perspectives:

1. Emergency or fault management
2. On-going operational support management (monitoring)

Fault management will be undertaken by the organization that is primarily responsible for managing the interconnection (COMPANY A). It is the responsibility of the managing organization to resolve the fault as expeditiously as possible, to communicate status of the connectivity to organizational management, and to facilitate the communications between vendors and other technical personnel.

On-going operational management support shall also be the responsibility of the organization that is primarily responsible for the connectivity (AFF). The organization primarily responsible for the connectivity will be responsible for:

- Change and configuration management
- On-going bandwidth utilization monitoring

The ASD and AFF technical staffs will manage the configuration of the hardware and software in accordance with AFF’s Change Management processes and procedures (provided by AFF), and by the IAS-LAN System’s Security Plan (SSP). Software configuration changes will be enacted after change requests are received and signed by the management of the interconnected organizations on appropriate request forms. See Table for the appropriate management signatory levels required for network change and configuration management requests at AFF.

Table 1 – AFF IT Management Staff with Roles and Responsibilities

Organization	Name	Responsibilities
ASD Chief	Rick Mills	Responsible for all IT Directorate activities. Authorizes emergency connectivity requirements using non-standard connectivity methodologies.
AFF Technical Specialist	Neil Flagg	Responsible for AFF Data. Authorizes all requests for standard connectivity and recommends approval of all non-standard connectivity methods.

7. Costs

There are no ASD or AFF-based costs associated with this ISA.

8. System Security Considerations

- **Services Offered:** No user services are offered. This connection only exchanges data between COMPANY A’s system and AFF’s system via a HTTPS data exchange protocol.
- **Data Sensitivity:** The sensitivity of the data exchange is **Sensitive-But-Unclassified**.
- **Incident Reporting:** The party discovering a security incident will report it in accordance with its incident reporting procedures. In the case of AFF, the incident will be reported to the ASD’s Computer Security Incident Response Team (ASD-CSIRT), by calling at 208-433-5049.

**Property of the United States Government
This Document Contains Sensitive But Unclassified
Information**

Do not remove this notice
Properly destroy when no longer needed

9. Signatory Authority

This ISA is valid for one year following the latest date of either signature below. At the end of this period the ISA will be reviewed, updated (if appropriate), and reauthorized. Either party may terminate this agreement upon receipt of 30 days advanced notice of intent to terminate or in the event of a security incident that necessitates an immediate response.

Company A

**Rick Mills. Chief
ASD, National Business Center**

Date:_____

Date:_____

**Property of the United States Government
This Document Contains Sensitive But Unclassified
Information**

Do not remove this notice
Properly destroy when no longer needed