CASE STUDY:
Identity and Access Management (IdAM) Security Framework for DCGS-A

The Distributed Common Ground System-Army (DCGS-A) is a data system that supports field intelligence, surveillance information, and situational awareness from sensors and other inputs. The DCGS-A system faces digital security and identity and access management (IdAM) challenges including:

- Multiple hardware and software platforms and interfaces
- Multi-level security
- Multiple security credentials and passwords
- Multiple protocols (e.g., SOAP, HTTP/S, REST, CAS)
- Lack of "thread of identity" across the security context

An optimal IdAM architecture supports an interoperable, heterogeneous environment, is simple to develop, and non-intrusive as possible. These benefits can lower the barrier of entry for community members and encourage involvement by service providers across DCGS-A that face significant resource constraints but still are required to integrate.

Jericho Systems has worked closely with key stakeholders to help define DCGS-A's IdAM Security framework based on industry standards. The IdAM Security Framework enables single sign-on (SSO) authentication, attribute-based access control (ABAC), and policy-based access control (PBAC) through the customized use of Jasig's open source Central Authentication Service (CAS) and Jericho Systems' EnterSpace Decisioning Service (ESDS).

The solution can interface with the government's Ozone Widget Framework (OWF), Tactical Attribute Store (TAS), Multi-Function Work Station (MFWS), and Lightweight Directory Access Protocol (LDAP).

COMPONENTS OF IDENTITY AND ACCESS MANAGEMENT SECURITY

Controlling access to digital services and data requires three main capabilities: authentication, authorization, and audit. **Authentication** identifies a user to the system. **Authorization** confirms that the user possesses security privileges and is entitled to access

the services and data. **Audit** capabilities provide a reliable record of user activities on the system and prevent false repudiation.

A flexible, robust IdAM framework for DCGS-A includes:

- Configurable authentication able to support Active Directory (AD) with other LDAP directories and/or PKI, plus ability to propagate identity across multiple tiers within a multi-tiered topology.
- Mechanisms that evaluate and authorize access requests based on configurable digital policy (for policy-based access control, or PBAC).
- Mechanisms that dynamically retrieve and evaluate user attributes and environmental context from multiple data sources (for attribute-based access control, or ABAC).
- An architecture that includes a configurable policy enforcement point (PEP), policy administration point (PAP), and policy decision point (PDP).
- Extensible implementation that allows for domain- or Community of Interest (COI)-specific customizations.

ENSURING INTEROPERABILITY AND FUSION OF DATA SOURCES

DCGS-A programs must interact with other DCGS services and the wider intelligence community to share IT services, intelligence, and digital content. Jericho Systems supports the DCGS-A IdAM solution using open standards that allow interoperability, extensibility, and vendor independence across Army mission domains.

DCGS-A SOFTWARE BASELINE (DSB) RELEASE IDAM ARCHITECTURE

Jericho Systems supports the baseline release with various IdAM components within DCGS-A's Work Server Suite (WSS) and Basic Analyst Laptop (BAL), including: authentication and single sign-on (SSO) support for Web applications, Ozone widgets, Multi-Function Work Station (MFWS), RESTful and SOAP-based services, a REST interface for non-browser based applications, client libraries written in multiple languages, Java EE support, and user identity propagation. Active Directory (AD) provides the authentication user registry and the Tactical Attribute Store (TAS) manages application-level permissions. Spring Security and JAAS are also supported.

The authorization interaction pattern follows the DoD and IC Service-Oriented Architecture Security Reference Architecture.