Cyber Situational Awareness Analytical Capabilities (CSAAC) is a set of NIPRNet and SIPRNet solutions that will provide the ability to collect, analyze, visualize, and share DODIN & Mission Partner information for collaborative DODIN Operations and Defensive Cyberspace Operations. CSAAC enables greater visibility into the enterprise allowing critical decisions to be made based on a richer and broader set of information. The Rapid Deployment Kit (RDK) is the big data solution that supports the data ingest, correlation, and visualization infrastructure.

Supporting the operation and defense of the Cyber mission space
**Collect Information**

**Analyze**

**Visualize**

**Share**

**UNCLASSIFIED**

**Functional Components**

---

**Mission Planning**

**Continuous Risk Management**

**Network Management**

**Enterprise Service Management**

**Cyber Defense Near Real and Real Time**

**Cyber Information Sharing**

---

**ANALYTIC PLATFORM**

**DATA INGEST SERVICE**

**DATA SOURCES**

---

**DISN C3S**

**JCSS**

**Commercial Cloud**

**Federal**

**CCDC/DECC**

**Gateways**

**Enclaves & End Points**

**Intel**

**DIB**

---

**DODIN, Federal, and Mission Partner Enterprise Environment**

---

**UNCLASSIFIED**
Supports Multiple Mission Sets to Enhance Decision Support

**Analytics User Base**
- DISA Command Center, OPS, CONUS, EUR, PAC, EIS, STRATCOM, JSSC, EE, Ent Ops
- NORTHCOM, SOUTHCOM DECCs: OKC, MECH, ESD-NA
- CYBERCOM ACOIC, 561st NOS DOK Joint Staff, NSA, IAD, OSD, NTOC, HQDA/ITA, HQ Air Force
- NETCOM, ARCYBER, TRANSCOM, Army CIO/G6 USTRANSCOM, AFCYBER USSOUTHCOM, JFHQ DoDIN DES Community

**Metrics**
- 15 ingested data sources
- 102 deployed widgets
- 747+ users

**DODIN Ops / Situational Awareness**
- Defense Enterprise Email Monitoring

**Defensive Cyber Ops**
- Fight By Indicator (FBI)

**Audit Management**
- Insider Threat Detection Service

**Mission Mapping / Continuous Monitoring**
- Roadmap Capability
# CSAAC-RDK Operational Overview

## What is CSAAC-RDK?

- CSAAC-RDK is a DISA developed capability for ingesting and storing large data sets, building analytics, and visualizing the results.
- Allows critical decisions to be made based on a richer and broader set of information.
- Developed around open source and unclassified components while leveraging community tech transfer from other DoD entities.

## CSAAC-RDK within DISA

- Production environments deployed on NIPR, SIPR, and a Private Secret enclave.
- Environments available in JITC lab for mission partner development.

## CSAAC-RDK Key Objectives

- Aggregate DoD data to operate, assure, and defend the DODIN
- Support JIE & JRSS initiatives of data collection and analysis
- Enable collaborative analytic development across the DoD
- Establish governance aligned with operational requirements

## CSAAC-RDK Mission Partners

- CSAAC-RDK has been embraced by multiple mission partners including USCYBERCOM, NSA, Army, Navy, Air Force, and the Marines.
- CSAAC-RDK allows mission partners to rapidly meet the demands of their mission (e.g. ARL’s mission to operate and defend the DREN).
Integrated Architecture

RDK provides the potential to consolidate CSAAC capabilities.

This is only an example.
CSAAC-RDK Strategic Linkages

- Standards
- Governance
- Consolidate IT
- Joint Operations

- Data Collection
- Analytics
- Visualization
- Info Sharing

Enhance Shared Situational Awareness (ESSA)
**Path Toward Convergence**

**Present Efforts**
Developing a unified architecture with common APIs, data schemas, and data standards

**Future Efforts**
Integrate CSAAC-RDK with the Intelligence Community and Navy Tactical Clouds
Vision: Cross domain capabilities

Coast Guard Cyber

Service / National Research Labs

NSA & CYBERCOM

ARCYBER

“Query one, query all”
Industry’s Role with CSAAC-RDK

There are three predominant opportunities for Industry big data participation:

1. Create solutions that can seamlessly integrate into the existing big data infrastructure and augment / enhance currently deployed capabilities

2. Develop solutions that support big data analytics which can be shared amongst all agencies and enhance collaboration

3. Bring your COTS solution:
   - Attributes of a COTS tool to be considered as an enterprise solution should provide capabilities that:
     - Satisfy validated DOD operational requirements
     - Are not redundant with currently deployed capabilities
     - Offer a more cost effective solution which would be too time consuming or expensive to build ourselves on CAAC-RDK
     - Integrate with existing CSAAC-RDK infrastructure
Contact/POC Information

Information
www.disa.mil

Website or Program External Link
https://east1.deps.mil/disacop/maenetops/CSAAC/SitePages/Home.aspx

EMAIL

Robert Landreth – Program Manager
Robert.Landreth2.civ@mail.mil