

# DETECTION & ASSESSMENT

Designed to Federal Specifications

The ability to detect an adversary and assess their intentions is a fundamental physical security tenet. This capability area addresses the design of equipment to identify and warn of unauthorized access to a specified site or installation as well as equipment related to the notification and identification of explosive threats or hazards.

## **Definition: Risk-Adaptive Insider Threat Intelligence & Interception (RAdInT)**

Security investigation decisions are supported and executed based on a combination of a user's role, mission need, and the level of security risk that exists between the facility being accessed and the current user of credentials.

## **Risk-Adaptive Insider Threat Intelligence & Interception (RAdInT)**

Risk-Adaptive Insider Threat Intelligence and Interception (RAdInT) system provides enterprise-wide monitoring and enforcement capabilities for the prevention, detection and mitigation of physical Insider Threat (InT) attacks.

RAdInT modernizes installation security postures against unauthorized physical access, including rogue badges and operator collusion. Using risk-based analysis and riskadaptive controls, decision-makers can more effectively prevent, detect, investigate, mitigate and report suspected physical InT activity. For the first time, security operations are capable of verifying fitness and evaluating the purpose surrounding physical access requests based on real-time situational awareness data.

RAdInT was designed to improve operational effectiveness, installation resilience and threat detection capabilities for military-grade facilities using commercial off-the-shelf components (COTS).



## **RECONASENSE Requirements**

- APL #10131
- HSPD-12
- FIPS 201
- FIPS 140-2
- ICD705
- UL1076



## **Considerations From Defense Contractor Management Agency**

- Risk-based Analysis
- Risk-based Mitigation
- Risk-based Reporting Safeguards

## About ReconaSense

ReconaSense® is the first COTS risk-adaptive framework with FICAM certification that can uniquely help identify Insider Threats via real-time data transformation, evaluation and automated policy adjustments. We protect federal, military, state, and other critical infrastructures requiring top-grade security with insider threat detection and our unification platform.

ReconaSense is privately held company headquartered in Austin, Texas. Visit [www.reconasense.com](http://www.reconasense.com) to learn more.

Interested in a demonstration?

Email us at [insider@reconasense.com](mailto:insider@reconasense.com) or call us at **+1 512.220.2010**.

## Location

### CORPORATE HEADQUARTERS

9130 Jollyville Road  
Suite 150  
Austin, TX 78759



© 2021 ReconaSense.  
ReconaSense is registered trademarks of Tranquility Ventures.  
All other trademarks are the property of their respective owners.



ReconaSense is an American company  
headquartered in Austin, Texas.