DEFENSE INTELLIGENCE AGENCY

Insider Threat Program

10 September 2019

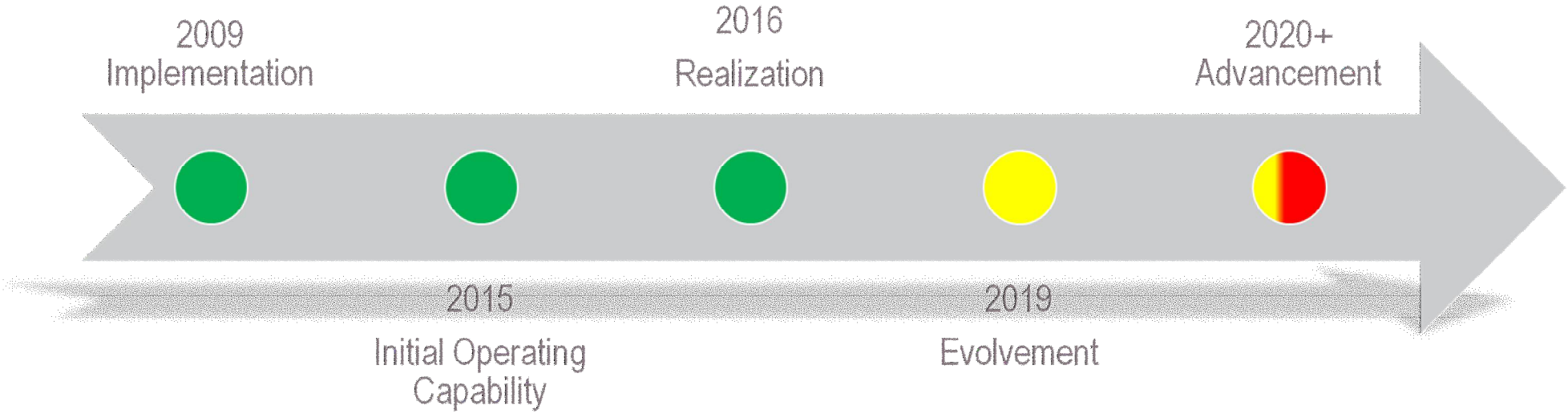
INSIDER THREAT PROGRAM STRATEGY OVERVIEW

INSIDER THREAT PROGRAM OVERVIEW

- Past
- Present
- Strategy
- Future

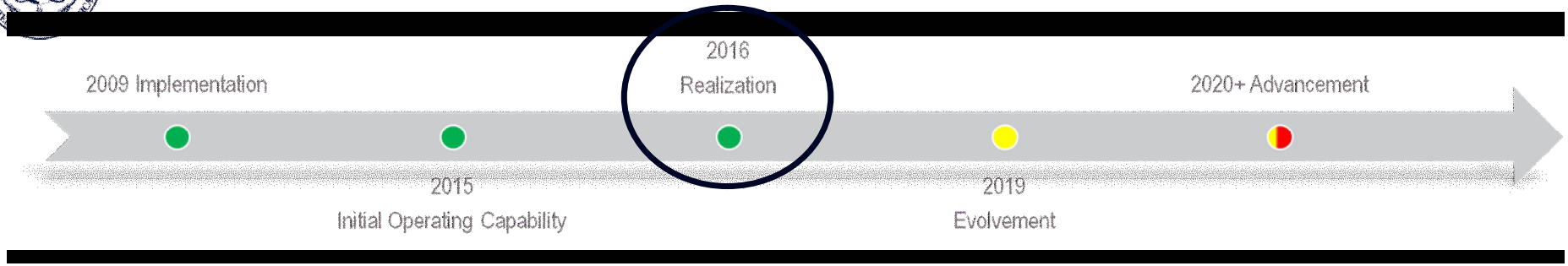
INSIDER THREAT PROGRAM TIMELINE

[redacted]



[redacted]

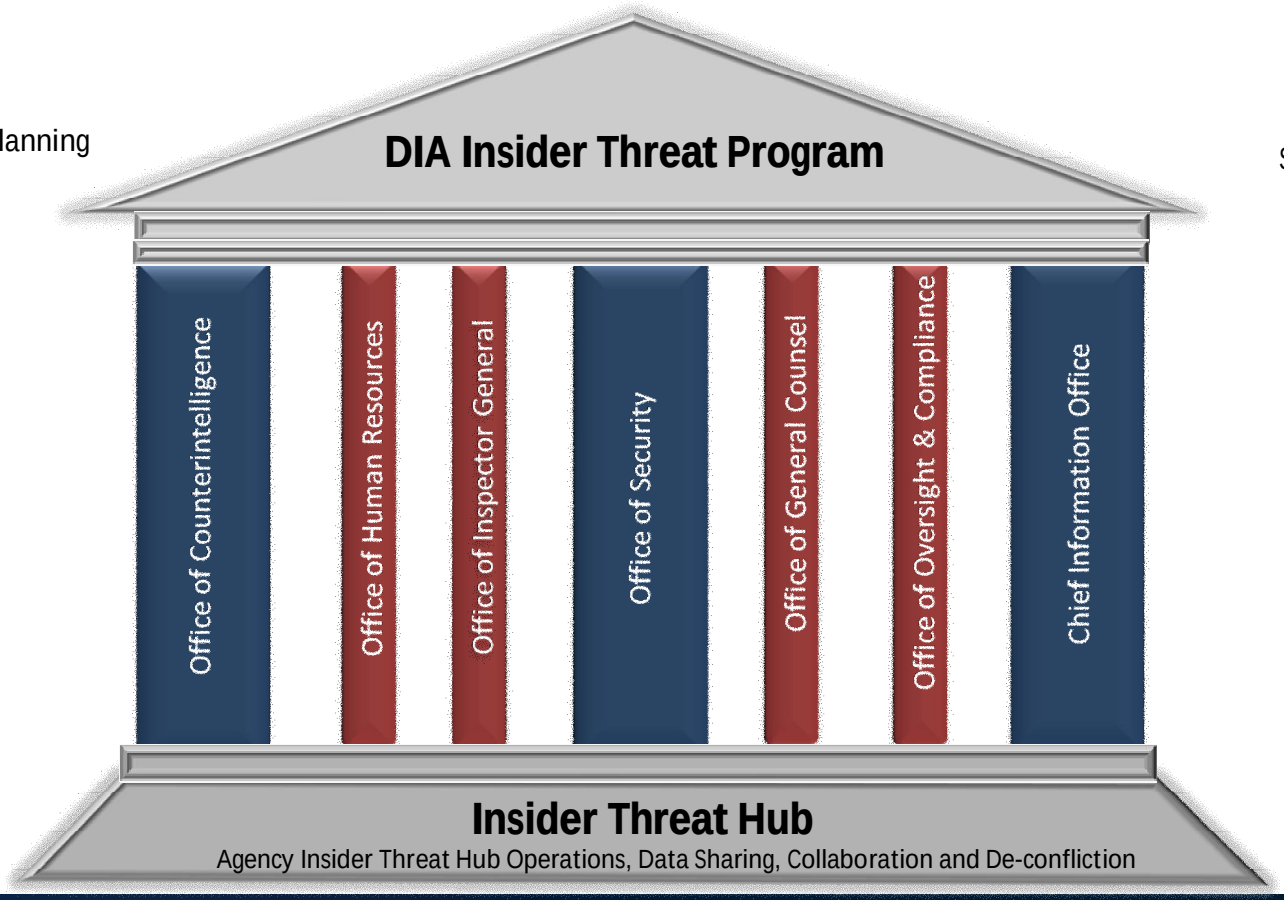
EXECUTIVE COMMITTEE DECISION

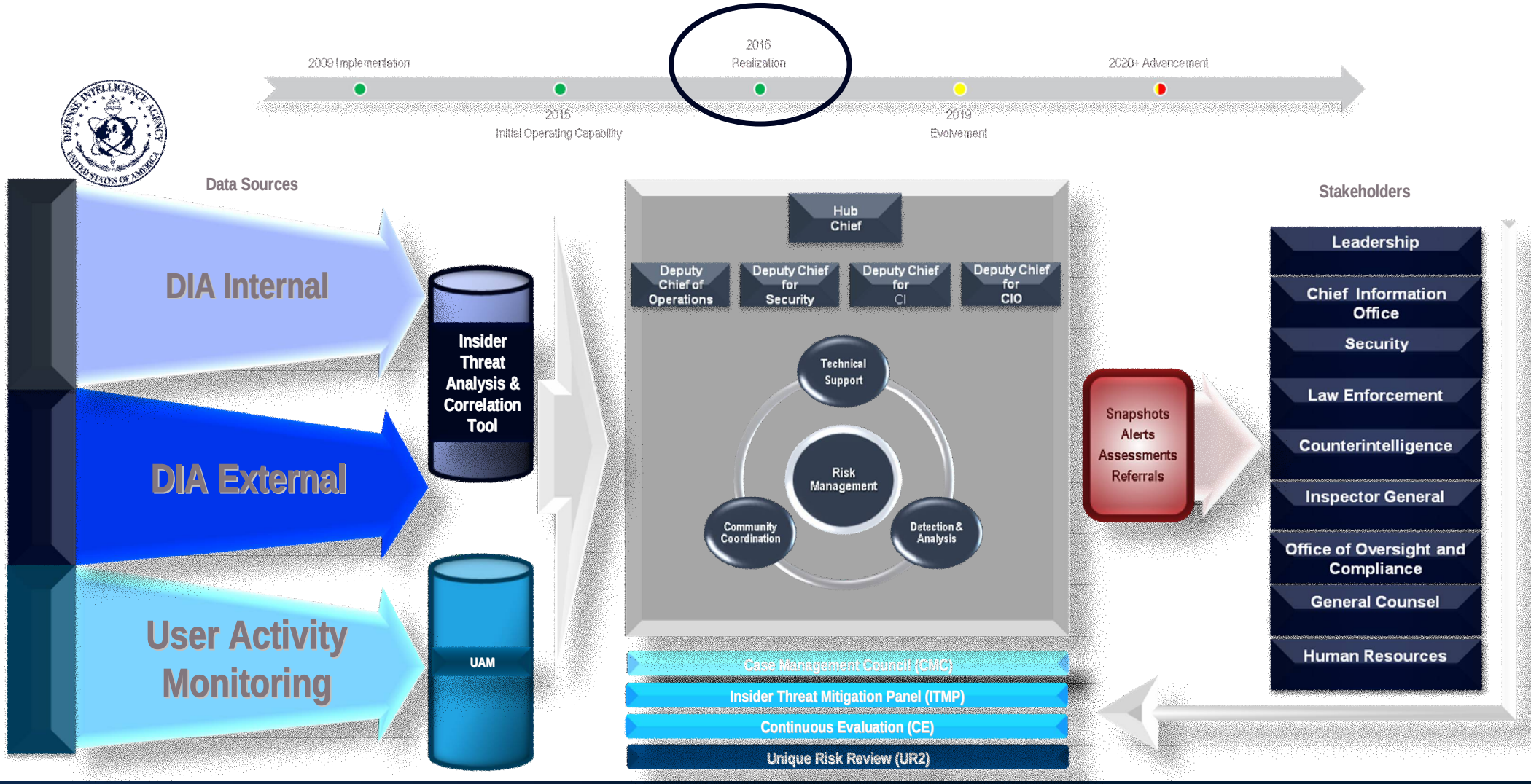


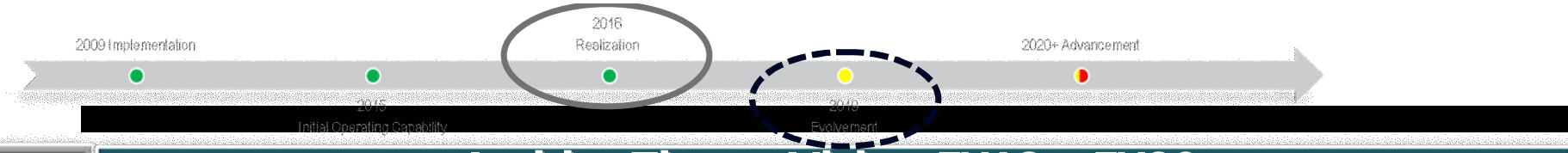
- Insider Threat Program (InTP) Hub Model
- Key Stakeholder Deputy Assignment
- Alignment of Security and Insider Threat Policies

Whole of Agency Strategic Planning and Oversight

Senior Designated Official




2009 Implementation
2015
Initial Operating Capability
2016
Realization
2019
Evolvement
2020+ Advancement
Data Sources
DIA Internal
DIA External
User Activity Monitoring
Insider Threat Analysis & Correlation Tool
UAM
Hub Chief
Deputy Chief of Operations
Deputy Chief for Security
Deputy Chief for CI
Deputy Chief for CIO
Technical Support
Risk Management
Community Coordination
Detection & Analysis
Case Management Council (CMC)
Insider Threat Mitigation Panel (ITMP)
Continuous Evaluation (CE)
Unique Risk Review (UR2)
Snapshots
Alerts
Assessments
Referrals
Stakeholders
Leadership
Chief Information Office
Security
Law Enforcement
Counterintelligence
Inspector General
Office of Oversight and Compliance
General Counsel
Human Resources



Insider Threat Vision FY18 – FY20

DIA's Insider Threat Program (InTP) will continue to be a top-tier program benchmarked by other Agencies within the DoD and IC. The DIA InTP, which has reached FOC, has a well-trained workforce who not only understand the mission, but are also active participants in a program that prides itself on its ability to detect, deter and mitigate threats posed to the Agency. DIA's InTP also continues to contribute to the Community through effective outreach efforts assisting other programs by providing them with insight into its policies and procedures, best practices, and lessons learned.

Key Enablers: Process – Documentation – Policy – Leadership – Resources – Trends

Insider Threat Roadmap FY18 – FY20

JUN 2018 – MAY 2019
"Setting the Foundation"

Develop Business Process/procedures

Educate DIA Workforce (Strategic Communications)

Tiered Certification Levels – Insider Threat Workforce

Enhance Predictive Analysis

Reach National Insider Threat Task Force (NITTF) FOC

Next 18 = JUN 2019 – SEP 2020
"What it Means to be The Hub"

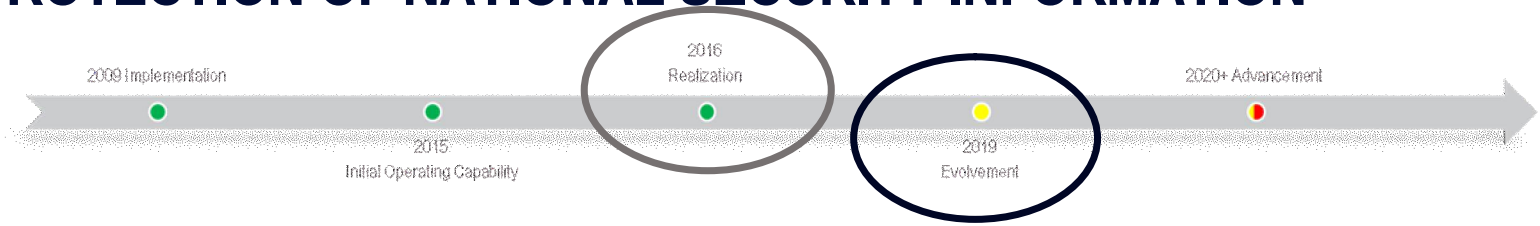
Refine Insider Threat Program Workforce

Innovate Technically & Operationally

Strengthen Stakeholders & Outreach

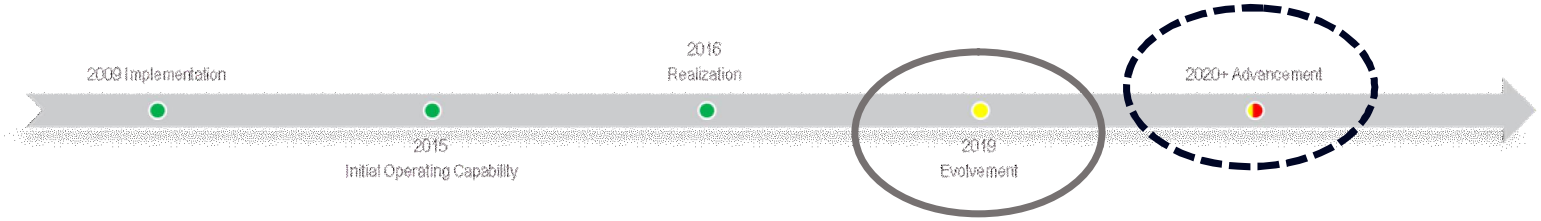
Key Insider Threat Community Integration

PRESENT: BALANCING CONSTITUTIONAL RIGHTS WITH THE PROTECTION OF NATIONAL SECURITY INFORMATION



- Characterization of DIA's Insider Threat Program
- 4th Amendment and handling of Cache Data
- 1st Amendment and Baseline and Enhanced Triggers
- Atypical Communications (i.e. Privileged Communications, 3rd Party Communications)
- Data handling, retention and dissemination
- Use of outside data streams

FUTURE: INSIDER THREAT PROGRAM ACTIONS



- Continue building insider threat workforce skills consistent with DIA's talent management program
- Expand access to new data sources
- Apply greater use of available technologies to identify threats earlier
- Achieve FOC consistent with the NITTF standards

DEFENSE INTELLIGENCE AGENCY

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION