Threats to Cleared Industry through Cyberspace

OVERALL CLASSIFICATION: UNCLASSIFIED

Todd Tucker
Chief, Program Integration
Counterintelligence (Cyber)

April 2014

The Threat

Who is targeting?

- Foreign state sponsored actors
- Foreign intelligence entities (FIE)

What is targeted and how do they collect?

- Target U.S. Department of Defense critical programs – Personnel and Technology
  - Targeting scope is constantly unfolding
  - Actors are relentless

Past vs. Future

The adversary controls time, place and means

Cyber attacks occur with or without industry self-reporting

If your next project is aligned with the problems, needs, or desires of the adversary; or if your defenses are weak –

ARE YOU A TARGET?

What do FIE want?

How does DSS preempt FIE?

When you change the way you look at things, the things you look at change.

– Max Planck (Nobel Physicist)

Defense Security Service

Using Cyber to our Advantage ?

Landscape:

- Network Defense is a one part of the strategy
- Threats begin and end with a human
- Cyber Intelligence must be presented in a holistic fashion (threat, vulnerability and value)
- 70% of all Counterintelligence case referrals by DSS involve cyber activity

Anticipatory Analysis:

- Left of the cyber "boom;" get ahead of the threat
- The infectious spread? The "spider web" in Cyberspace interconnected
- Indicators begin with: Cyber Incident and/or Consequence/Value
- Relies on Cleared Contractor Self-Reporting

Using Cyber to our Advantage (cont)?

Reporting matters:

- Identifies the threat to specific technology
- Develop actionable information
- Articulating the threat
- NISP required reporting

DSS Counterintelligence (Cyber) Division

- Weekly Cyber Activities Brief posted to: https://HSIN.DHS.GOV
- Contact DSSCYBERCI@dss.mil

www.DSS.mil

Defense Security Service

Questions

www.DSS.mil

https://twitter.com/DSSPublicAffair

https://www.facebook.com/DSS.Stakeholders