DoD Office of General Counsel

DIB Pilot Legal Construct & Framework Agreements

07 July 2010

(b) (6)

Associate General Counsel

Overview

- Overview of the Legal Construct
- The Partnering Triangle
- Framework Agreement Elements That Are Not Affected
- Sharing the Enhanced Threat Information Products
- Event Reporting and Sharing of Information
- DIB Partner Informed Consent
- Questions?

The Legal Construct

Voluntary

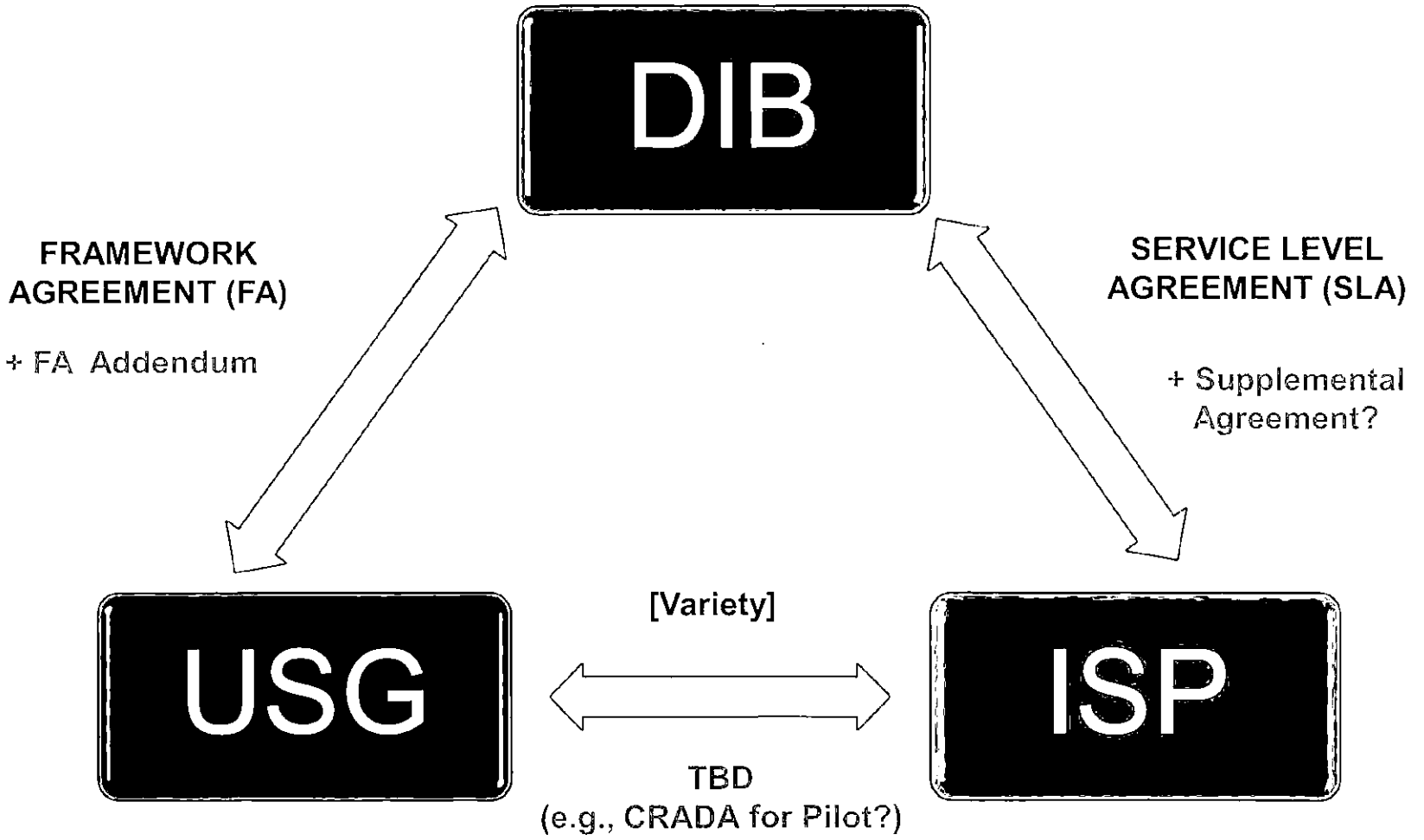
Informed

Consent

The Legal Construct

- **Basic Authority: DoD Information Assurance**
  - DIB Cyber Security/Information Assurance Program
  - Critical Infrastructure Protection Activities
- **Leverage existing relationships, mechanisms**
  - Add new benefits – supplementing the current state
- **Avoid legal obstacles to detecting, reacting, sharing information regarding malicious cyber events**
  - Constitutional: 4th Amendment
  - Statutory: Wiretap Act, Stored Communications Act, Computer Fraud & Abuse Act, Pen/Trap & Trace
  - Contractual: effect on existing obligations, restrictions
- **Voluntary, Informed, Consenting, Partnership – "Opt In"**

The Partnering Triangle



FA Elements NOT Affected

- **Government Threat Information Products** currently provided . . . and being improved continuously
- **DIB Partner Reporting** of Tier-1 or -2 cyber intrusion events
- **Follow-up → Detailed Forensics & Damage Assessment**
- **Protection for Shared Information**
  - E.g., Attribution Information, FOUO/Classified threat info

The Enhanced Threat Information Products

- **Additional, classified threat information products**
  - Example: TS/SCI signatures, actionable info, countermeasures
  - Not available from other sources
  - Not available under the current FA sharing mechanisms
  - For the Pilot: limited to two specific types of countermeasures

- **Goal: minimize deployment profile/exposure** – in reaching the maximum number of DIB Partners

- **Products provided directly to DIB Partner ISP(s)**
  - Deployed in a secure, USG-approved
  - Applied to consenting DIB Partner internet traffic
  - Enhancement to existing ISP services

Reporting & Sharing of Cyber Event Information

- **Enhanced Products** – enable automated (configurable) detection, response, and reporting
  - Reacts ONLY to known, malicious events/criteria
  - Capability to engage and defeat the attempted malicious act

- **Reporting available to--**
  - DIB Partner
  - ISP
  - USG

- **Types of Reporting**
  - Real-time vs. periodic/aggregated
  - Detailed vs. aggregated or anonymized

DIB Partner Consent

- **Actual Consent is the CORE approach to avoid legal barriers to—**
  - Applying the countermeasures
  - Sharing the information regarding malicious events
- **DIB Partner "Entity" Consent**
  - Addendum to the FA with DoD – outlines the new process
  - Agreement with the ISP regarding effect on services
- **DIB Partner – "User's" Consent**
  - Example: logon banners, user agreements, training
  - DIB Partner certifies adequate procedures in place. . .

Notional FA Addendum Structure

- **Purpose:** Scope/purpose of the opt-in pilot
- **Definitions:** "Enhanced Threat Information Products" (classified appendix, if needed)
- **Sharing ETIPs:** Directly with designated ISP
- **Reporting:** Define nature, type, timing to DIB, ISP, USG
- **Express Consent:** for DIB entity, and ensuring DIB network users

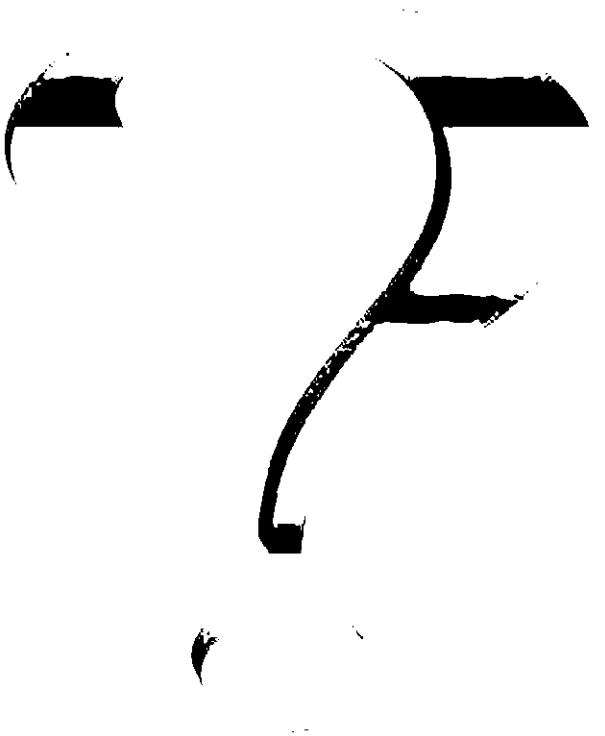
Questions?

Richard M. Gray

Associate General Counsel
Department of Defense
Office of the General Counsel

Direct: (b) (6)

NIPR: (b) (6)
SIPR: (b) (6)
JWICS: (b) (6)



BACKUP SLIDES

00955

Selected Legal References

- Information Assurance
  - 10 USC 2224, Defense IA Program; 44 USC 3541 et seq., FISMA
- Critical Infrastructure Protection
  - HSPD-7, Critical Infrastructure Protection
- Comprehensive National Cybersecurity Initiative
  - NSPD-54/HSPD-23
- Crimes Against Computers or Communications Systems
  - 18 U.S.C. § 1030, Fraud and Related Activity in Connection with Computers
  - 18 U.S.C. § 2510 et seq, Wire and Electronic Communications Interception and Interception of Oral Communications
  - 18 U.S.C. § 2701 et seq, Stored Wire and Electronic Communications and Transactional Records Access
  - 18 U.S.C. § 3121 et seq, Recording of Dialing, Routing, Addressing, and Signaling Information