Intrusion Detection and Prevention (What, Where, How and Who)

What, Where, How, and Who

What

- **.gov Intrusion "Prevention" (IPS)**
  - Decision Logic
    - We don't always want to prevent.
- **Enterprise Solution**
  - Common Standards
  - Shared Analytics
- **Take Advantage of Classified Info**
- **Share Information**
  - LE, IC, Military, International
  - Interoperability

Where

- **SCIF Facility (TS/SCI)**
- **Location**
  - Agency Level (too may)

OR

  - TIC (too many for now)

OR

  - ISP

OR

  - Network Exchange Points

How

- **Commercial Off The Shelf (COTS)**

AND/OR

- **Government Developed**

Who

- **USG (DHS/CIOs)**

AND/OR

- **Private Sector**
  - Managed Security Services

Legend

- Privacy Points of Interest
- Choices

Advantages for the Who

Advantages of the USG

- Ability to execute inherently governmental functions
  - Response decisions (prevent, monitor, notify?)
  - Consideration of all USG equities
- Promote central governance
- Instant access to conduct independent auditing and compliance, without requiring contractual agreement

Advantages of Private Sector

- Help protect the .gov by seeing what is happening on the .com
- Situational Awareness using both .com and .gov data
- Ability to determine unique effectiveness of using classified information, with ability to:
  - Determine scope of .com that is under attack but could be helped if .gov would share
  - feed into USG Vulnerabilities Equities Process (VEP) to promote sharing of Essential Elements of Information that would make a difference

Privacy

- Privacy Issues:
  - IPS signature development and use
    - How are signatures vetted prior to deployment?
    - Can it ever be automated?
  - Sharing log data with other communities?
    - How are events categorized and information shared for response?
    - Can it ever be automated?
  - Instrumenting the Net
    - Can the solution be used to help protect the critical infrastructure?
    - If so, we must protect against unauthorized use.

- Law / Process / Compliance
  - Executive Branch (Attorney General, Agency CLPOs and OGCs)
  - Congressional Oversight
  - Public debate
  - Independent review of security measures that could be easily subverted if released publicly.