# An Inside Look Into Defense Industrial Base (DIB) Technical Security Controls:

## How Private Industry Protects Our Country's Secrets

James Kirk

# Outline

- Background
- DOD Agency Responsible for Interpretation and Enforcement
- Security Control Development
- Document Drafting and Approval
- Testing of Security Controls
- Enforcement
- The fun stuff… gaps in security controls

# Background/Disclaimer

- What kind of data are we talking about?
- National Industrial Security Program (NISP) Executive Order 12829 [1.]
- National Industrial Security Program Policy Advisory Committee (NISPPAC)
- National Industrial Security Program Operating Manual (NISPOM)

1. DoD 5220.22-M “National Industrial Security Program: Operating Manual.”

# DOD Agency Responsible for Interpretation and Enforcement

- The Defense Security Service (DSS)
- Agency Structure
  - Directorates (IS, CI, DISCO, and CDSE)
  - ODAA
  - Field Offices

# Basics of Certification and Accreditation (C&A)

- What is C&A? [1., 2.]
  - Certification
  - Accreditation
  - ISSP role
  - RDAA role
- Enough background on the DSS, lets get into security controls

1. Industrial Security Field Operations (ISFO) Process Manual for the Certification and Accreditation Of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM) and NIST 800-53.
2. Master System Security Plan (MSSP) Template for Peer-to-Peer Networks.

# Security Controls

- Where do they originate from?
- Linux controls [1.]
  - Audit Areas

1. /bin
2. /usr/bin
3. /etc
4. /sbin
5. /usr/sbin
6. /var/audit
7. /usr/local
8. /opt
9. /home

[1.] ISL 2007-01

# Security Controls cont.

- Linux cont. [1., 2.]
  - DISA STIG vs NISPOM/DSS ISL

[1] Standardization of Baseline Technical Security Configurations.

[2] UNIX: Security Technical Implementation Guide.

| DISA STIG | DSS NISPOM/ISL |
|---|---|
| The SA will ensure audit data files have permissions of 640, or more restrictive. | (2) Audit Trail Protection. The contents of audit trails shall be protected against unauthorized access, modification, or deletion. |
| - Logon (unsuccessful and successful) and logout (successful) | (b) Successful and unsuccessful logons and logoffs. |
| - Process and session initiation (unsuccessful and successful) | (a) Enough information to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved. |
| - Discretionary access control permission modification (unsuccessful and successful use of chown/chmod) | N/A |
| - Unauthorized access attempts to files (unsuccessful) | (c) Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion. |
| - Use of privileged commands (unsuccessful and successful) | N/A |
| - Use of print command (unsuccessful and successful) | N/A |
| - Export to media (successful) | N/A |
| - System startup and shutdown (unsuccessful and successful) | N/A |
| - Files and programs deleted by the user (successful and unsuccessful) | N/A – Unless it's considered a "Security Relevant Object" |
| - All system administration actions | (d) Changes in user authenticators. |
| - All security personnel actions | N/A |

1. Standardization of Baseline Technical Security Configurations.
2. UNIX: Security Technical Implementation Guide.

# ISL 2009-01 and Windows Baseline Standards

- ISL 2009-01 [1.]
- Standardization of Baseline Technical Security Configurations – March 2009
  - This process manual is not directive in nature, but adherence to the standards in this process manual by NISP contractors is recommended in order for DSS to be able to expeditiously issue Interim Approvals to Operate (IATO) and Approvals to Operate (ATO).
- FISMA (NIST 800-53) - June 2011
- Linux left out (must be super secure on its own)

[1.] Standardization of Baseline Technical Security Configurations.

# ISFO Manual Updates (Summary of Changes) [1]

- Finally 14 character passwords required for all systems and 60 day change reqs.
- Patching is addressed now, in a semi-ambiguous way in section 5.2.8.1
    - The ISSM will identify ISs containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The ISSM will install security-relevant software upgrades (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously.

[1] ISFO Process Manual Revision 3: Summary of Changes.

# ISFO Manual Updates (Summary of Changes)[1]

- USB Drives Addressed… sorta.
- Audit requirements expanded on
  - 1. Enough information to determine the action involved, the date and time of the action, the system on which the action occurred, the system entity that initiated or completed the action, and the resources involved (if applicable).
  - 2. Successful and unsuccessful logins and logoffs.
  - 3. Unsuccessful accesses to security-relevant objects and directories.
  - 4. Changes to user authenticators.
  - 5. The blocking or blacklisting of a user ID, terminal, or access port.
  - 6. Denial of Access from an excessive number of unsuccessful login attempts.

[1] ISFO Process Manual Revision 3: Summary of Changes.

# ISFO Manual Updates (Summary of Changes) cont. [1]

- Security Seals…
  - Approved tamper-proof, pre-numbered seals should be used on hardware components (to include monitors and keyboards) anytime the hardware may be subject to access by uncleared personnel (i.e. used for periods-processing, or relocation).

[1] ISFO Process Manual Revision 3: Summary of Changes.

# Document Drafting and Approval

- ISFO Process Manual and Standardization Documents drafting
- Linux document development, and its death.

# Security Setting Testing

- Inadequate Labs
- Test Resources Limited

# Enforcement

- The Special Agent
  - The 0080 (Industrial Security Specialist) and 2210 Specialties (IT Specialist)
  - Training and authority
  - Subjectivity

# Enforcement cont.

- Inspection selection and process
  - Size of facility and complexity
  - “Partners with Industry”
  - What happens if non-compliance

# Inadequate Controls - Windows

- Patching [1.]
- USB
- Virtual Environments
- UAC
- Admin actions not audited
- Classified data not audited
- Tamper Controls

[1.] Standardization of Baseline Technical Security Configurations.

# Inadequate Controls - *nix

- Lack of expertise and training in agency leads to ostrich effect. [1.]
  - Job listings do not require any Unix or Linux experience.
- List is too long to list of files/services/versions that are not addressed.
  - Make it easy on themselves and use one of the configuration guides already in use.
- Auditing Rules not required to be in use in Red Hat… really?

[1.] Standardization of Baseline Technical Security Configurations.

# Inadequate Controls- *nix cont.

- Same issues affecting Windows, affect the Unix/Linux environment as well. [1.]
  - Patching
  - USB
  - Virtualized Environments
  - Auditing
  - Tamper Controls

[1] Standardization of Baseline Technical Security Configurations.

# Wrap-up

- So… why the talk?
  - Education… how many actually know how the U.S. protects classified data at the collateral level?
  - Enlightenment
    - I think it’s important to bring issues that are detrimental to the nations security to the forefront. These issues have been brought up to the agency, and ignored.
  - STUXNET and Flame…

# References

DoD 5220.22-M "National Industrial Security Program: Operating Manual." Department of Defense: Under Secretary of Defense for Intelligence. (2006).

"Industrial Security Field Operations (ISFO) Process Manual for the Certification and Accreditation Of Classified Systems under the National Industrial Security Program Operating Manual (NISPOM) and NIST 800-53." Washington DC: Department of Defense: Defense Security Service. (2011).

"ISFO Process Manual Revision 3: Summary of Changes." Defense Security Service Office of the Designated Approving Authority. (2011).

"ISL 2007-01." Department of Defense: Defense Security Service, Industrial Security Program Office. (2007).

"Master System Security Plan (MSSP) Template For Peer-to-Peer Networks." Defense Security Service Office of the Designated Approving Authority. (2011).

"SIPRNet Contractor Approval Process (SCAP)." Department of Defense: Office of the Designated Approving Authority. (2011).

"Standardization of Baseline Technical Security Configurations." Defense Security Service Office of the Designated Approving Authority. (2009).

"UNIX: Security Technical Implementation Guide." Defense Information Systems Agency. (2006).