

UNCLASSIFIED



Security Benchmarks

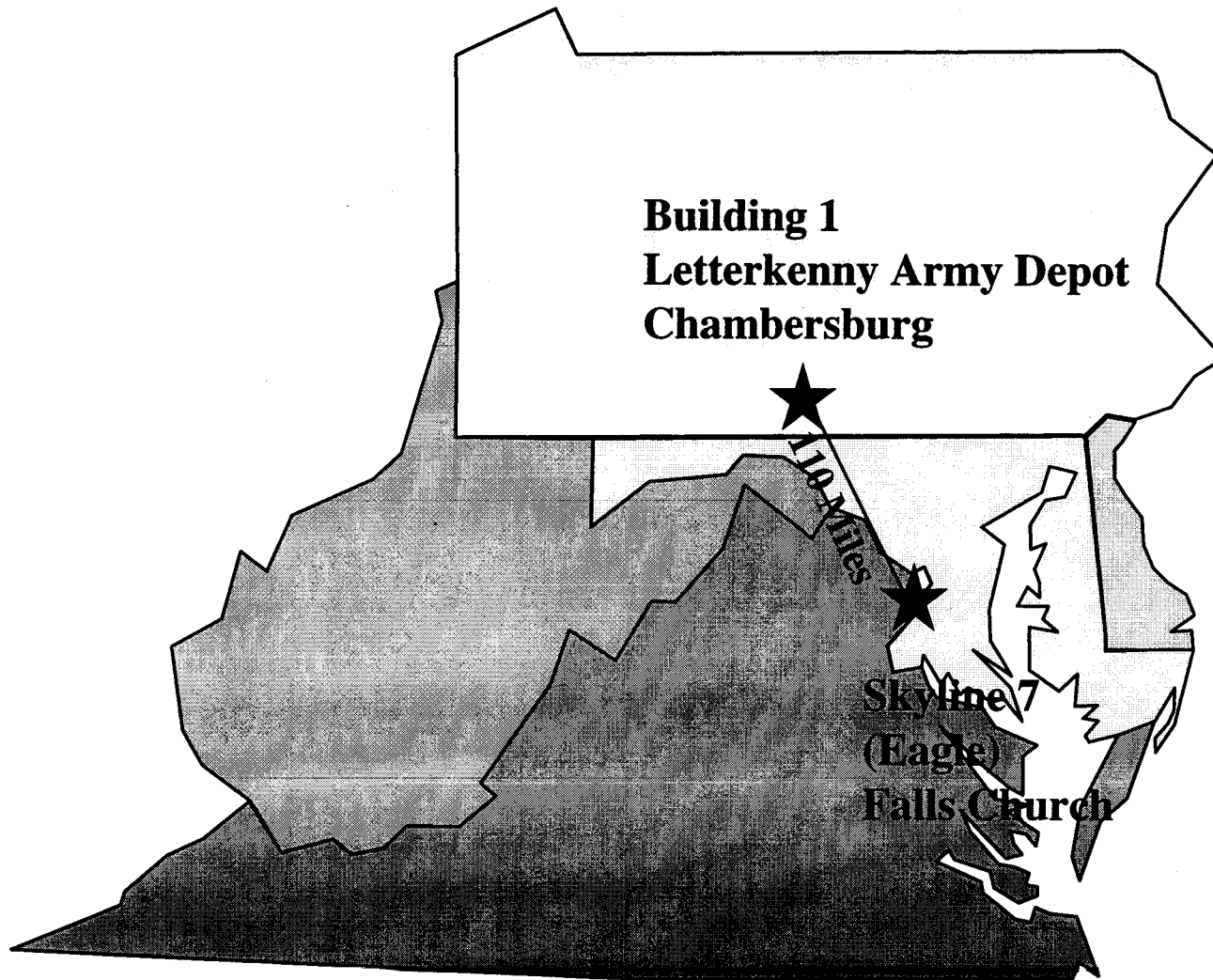
Terry Sherald
sherald@ritchie.disa.mil
717-267-9969
11 June 2003

UNCLASSIFIED



Unclassified

Where We Are



Unclassified



Unclassified

WHAT is a STIG?



- **Security Technical Implementation Guide:**
 - A Compendium of Security Regulations and Best Practices for Securing an Operating System or Application Software
 - A Guide for Information Security
 - Use is Mandated in by DISA Instruction 630-230-31
 - Authorized DODD 8500.1
- **GOALS**
 - Intrusion Avoidance
 - Intrusion Detection
 - Response and Recovery
 - Security Implementation Guidance

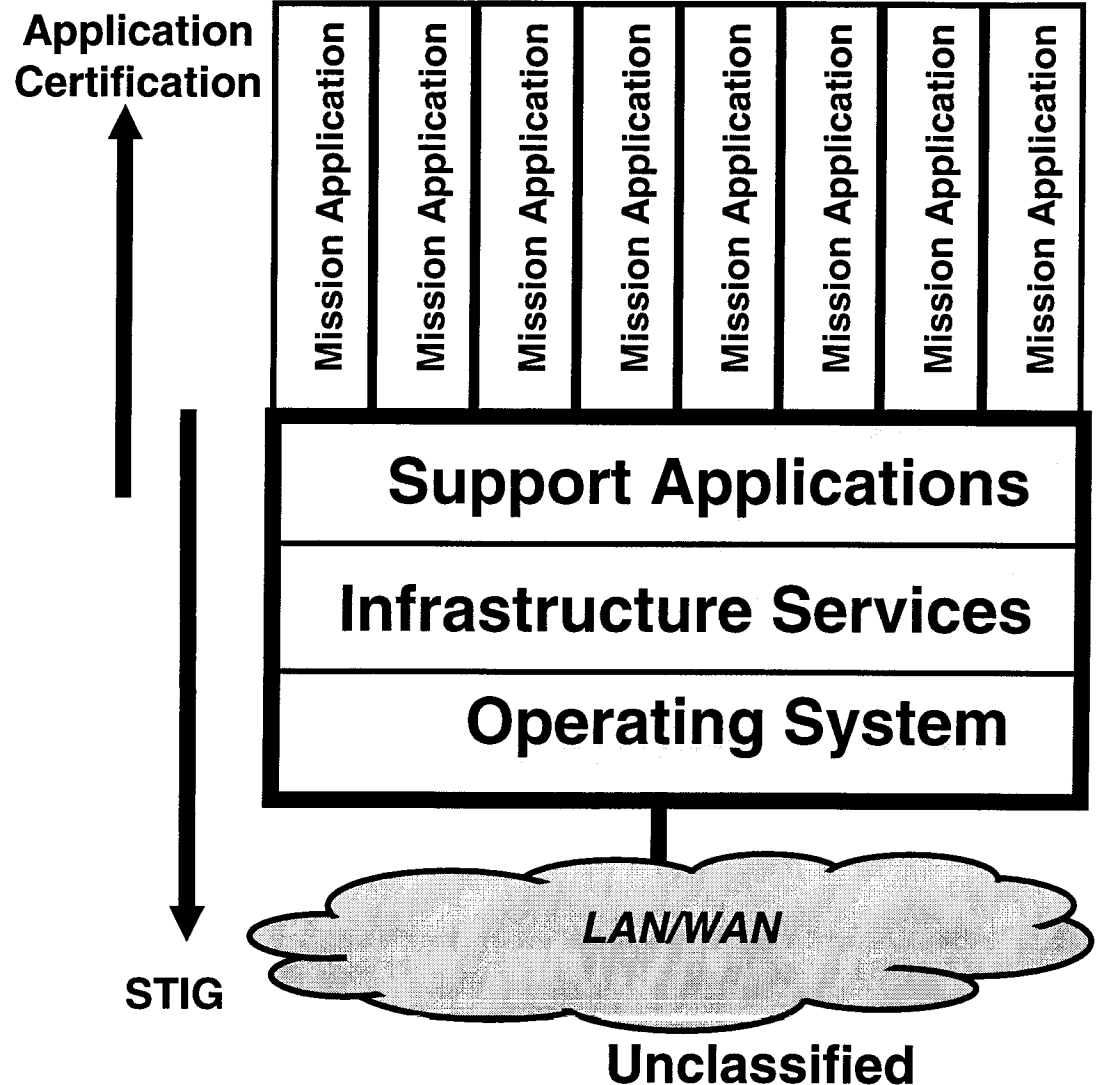
Unclassified



Unclassified

STIG Scope

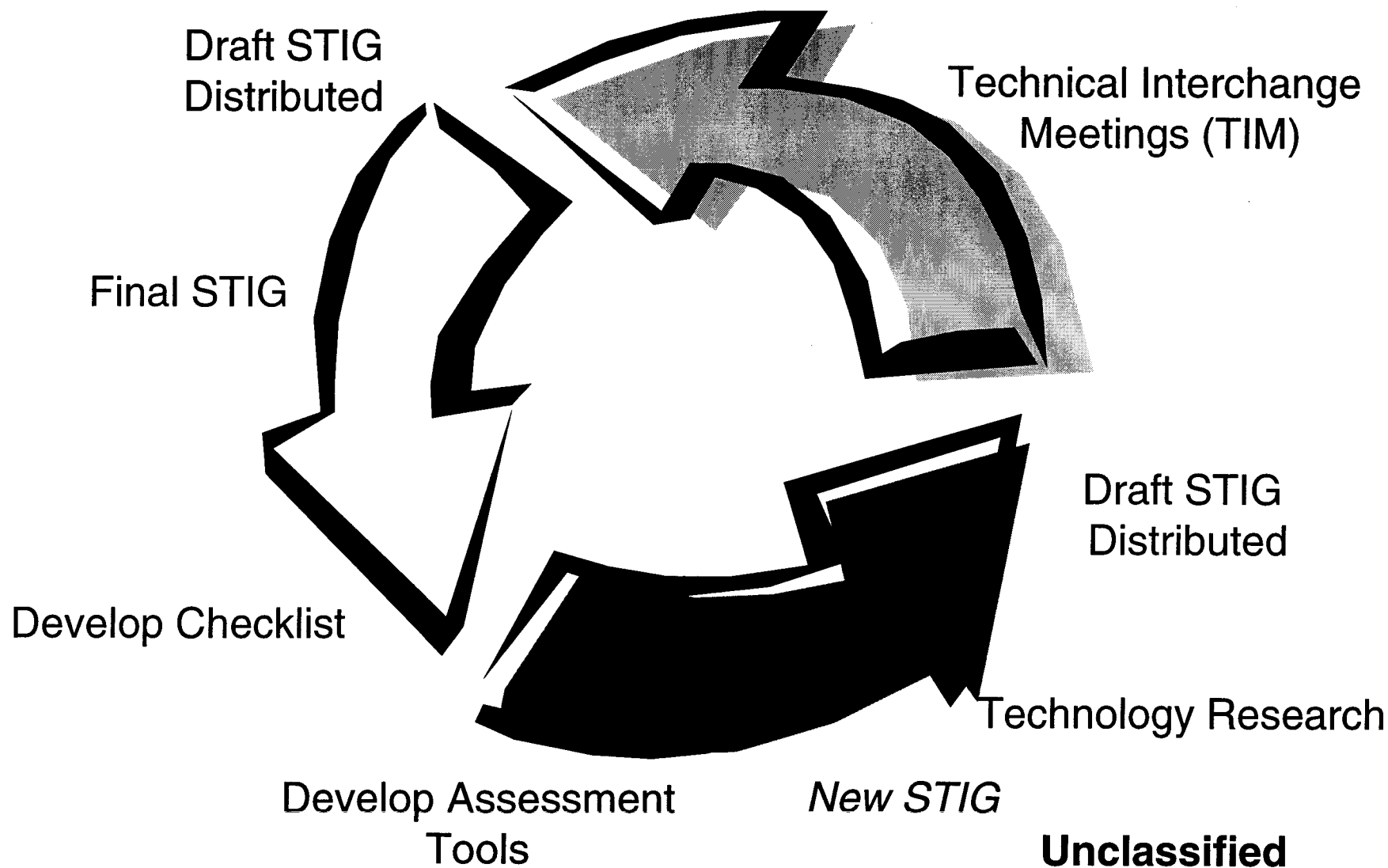
- Provides Standard, Secure environment for application development and operation
- Does not replace requirement for application security policy
- DISA is developing an Applications Developer Guide





Unclassified

STIG Lifecycle





Unclassified

DISA Security Technical Implementation Guides (STIGs)

- **NETWORK/PERIMETER**

NIPRNet

Enclave

Network Infrastructure

Wireless

DNS

Secure Remote Computing

- **OPERATING SYSTEM**

OS 390 (MVS)

VM

LPAR

Unisys

Tandem UNIX

Novell

Win NT (NSA)

Win 2K (NSA)

Win XP

Win NT/2K Addendum

- **APPLICATION**

Database

Web Services

Desktop Applications

- **USER**

Security Handbook

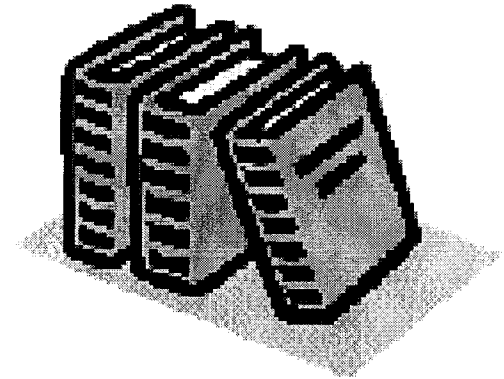
- **AVAILABLE AT THE FOLLOWING WEB SITES**

<https://iase.disa.mil>

<http://iase.disa.smil.mil>

<http://guides.ritchie.disa.mil> (Uses PKI cert or userid/password)

Contact FSO Support Desk for access – fso_spt@ritchie.disa.mil



Unclassified

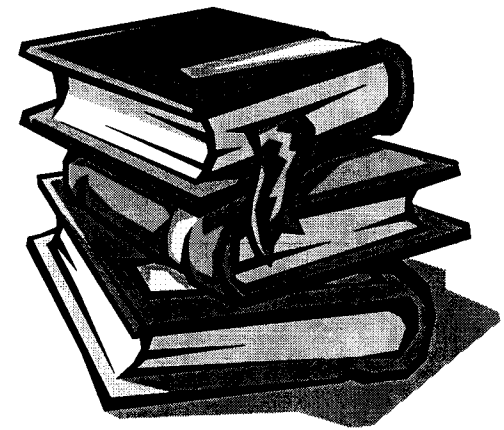


Unclassified

Draft/Future STIGs

•Current Drafts

- Network Infrastructure
- OS/390
- Logical Partition (LPAR)
- Virtual Machine (VM)
- Tandem
- UNISYS
- Wireless
- Database
- Web
- Enclave



•New STIGs in FY03

- Voice Over IP (VOIP)
- Optical
- Biometrics
- MAC

Unclassified

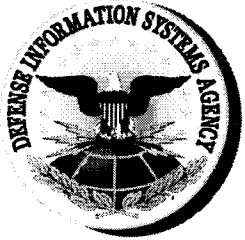


Unclassified

DISA Implementation

- **Gold Standard**
 - Applied to STIGs
 - Checklist
 - Scripts
 - Tools
- **Gold Standard Minimum Rqmt for Connection**
- **C&A Based on FULL STIG**
- **Gold Disk Tool**
 - Gold Standard Prototypes
 - Windows 2000 and XP
 - Solaris
 - Production Gold Disk (FUTURE)

Unclassified



Unclassified

Issues

-
- **Target Audiences (Home User, Corporate, etc.)**
 - **Gold Standard vs. FSO Gold Standard**
 - Specific DOD Issues
 - **Scoring Issues from CIS Tool**
 - Example: /etc/inetd.conf (Tool – no, STIG – yes)
 - What is a Vulnerability?
 - **Application Specific Issues**
 - Interoperability between Operating System and Application (I.e., Oracle) Security Settings
 - **Testing of Benchmark**
 - Difficult to Find Participants

Unclassified



Unclassified

Lessons Learned

- **Settings still Break Things**
- **Not enough time to be as active as needed**
 - Raising issues to the Benchmark (CIS)
- **Contingencies for Specific Settings**

Unclassified



Unclassified

Benefits

- **Vendor involvement**
 - Success Story - Microsoft Security Guide
 - Providing Direction to Vendors
- **STIG Improvements**
 - Documentation of Setting Keystroke fixes
 - Technical Resources and Expertise
- **Windows**
 - Starting to Focus on Non-native Environments vs. Native W2K

Unclassified