



UNCLASSIFIED//FOUO

Defense Security Service

Defense Security Service Cybersecurity Operations Division Counterintelligence



UNCLASSIFIED//FOUO



UNCLASSIFIED

Defense Security Service

DSS Mission

DSS Supports national security and the warfighter, secures the nation's technological base, and oversees the protection of U.S. and foreign classified information in the hands of Industry

CI Mission

DSS CI identifies unlawful penetrators of cleared U.S. defense industry and articulates the threat for industry and government leaders

Scope

- 10K+ firms; 13K+ facilities; 1.2m personnel
- 1 CI professional / 261 facilities
- 10.5% of facilities report

Capability

- (U) 11 personnel conducting analysis, liaison, field support, strategic development and program management
- (U) Wide range of skill sets – CI, CT, LE, Cyber, Security, Intel, IA, CNO and more
- (U) Direct access to cleared industry across 25 DSS field offices nationwide
- (U) Large roles at U.S. Cyber Command, National Security Agency, National Cyber Investigative Joint Task Force and the Department of Homeland Security

UNCLASSIFIED



UNCLASSIFIED

Defense Security Service

Challenges

- (U) Secure sharing of threat information with industry partners
- (U) Identifying and reporting suspicious network activity
- (U) Limited resources to execute for an quickly expanding mission area

Significant Achievements and Notable Events

- (U) Since September, 2009 – Assessed over 3,000 cyber-related suspicious contact reports from Industry and the Intelligence Community; facilitating action on over 170 federal investigations/operations
- (U) Developed four benchmark product lines for Industry and the Intelligence Community to include the 3rd edition of the DSS Cyber Trends
- (U) Briefed at 24 venues and over 1,000 personnel in FY12 on the cyber threat
- (U) In FY12, delivered over 350 threat notifications to industry, detailing adversary activity occurring on their networks.

UNCLASSIFIED

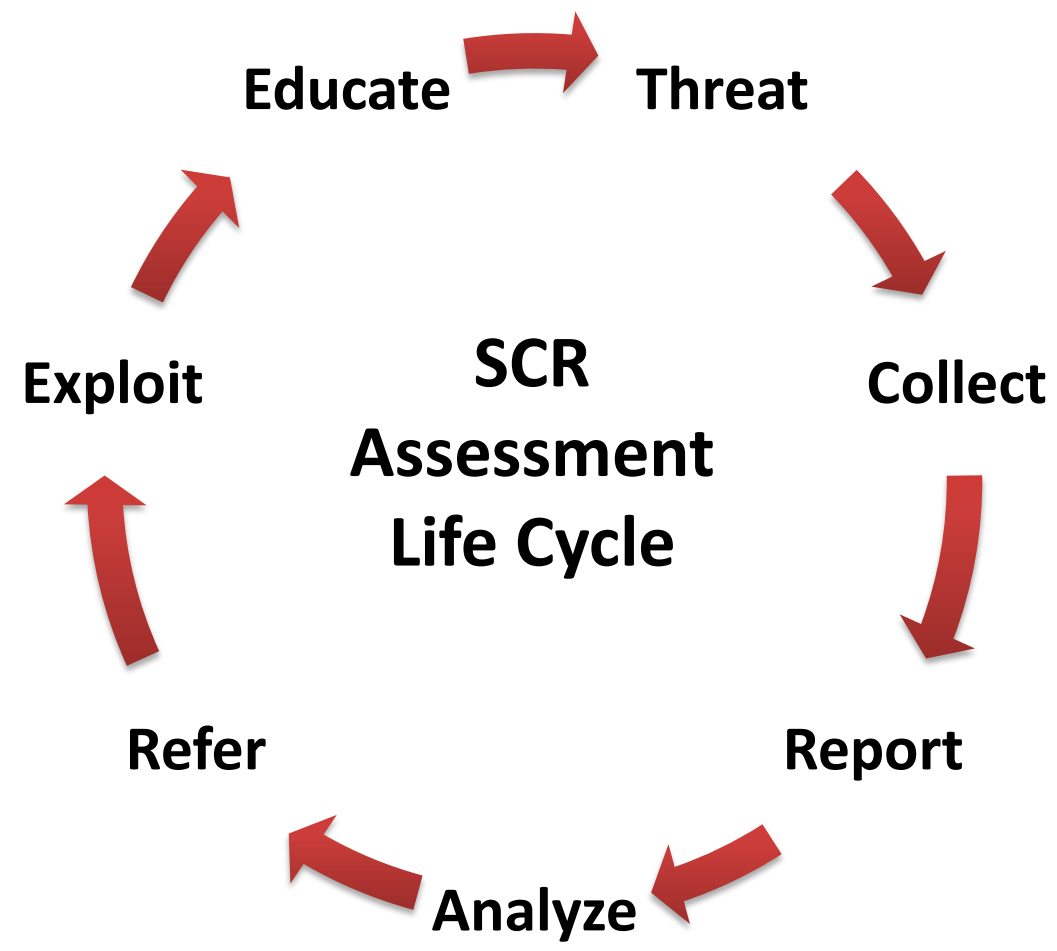


UNCLASSIFIED

SCR Assessment Life Cycle

Suspicious Contact Report

- (U) Fundamental building block of industry intelligence analysis
- (U) Highlights various methods of contact and approach
- (U) Provides vital insight to military programs and key facility programs



UNCLASSIFIED



UNCLASSIFIED

Evaluating Suspicious Contacts

Method of Operation

- Attempted Acquisition of Technology
- Conferences, Conventions, Trade Shows
- Criminal
- Exploitation of Relationships
- Seeking Employment
- Solicitation or Marketing Services
- Student Requests – Academic Solicitation
- Suspicious Network Activity

Collector Affiliation

- Commercial, Government, Government Associated, Individual

Technologies and Programs Targeted

- Military Critical Technology List

UNCLASSIFIED



Way Ahead

- (U) Continue to grow and expand DSS's cyber capability
- (U) Increase Opportunities for sharing of timely threat information and actionable data
- (U) Continue to build partnerships throughout cleared industry, intelligence and federal government communities





BREAK



UNCLASSIFIED//FOUO

Defense Security Service

(U) Cyber Threats to the Defense Industrial Base



UNCLASSIFIED//FOUO



- (U) Fiscal Year 2012 Industry Cyber Reporting
- (U) Threat Overview
- (U) Where We Are Vulnerable
- (U) Methods of Operation
- (U) A New Approach to Threat Modeling
- (U) Reporting
- (U) Getting Ahead



UNCLASSIFIED//FOUO

(U) FY12 Industry Cyber Reporting

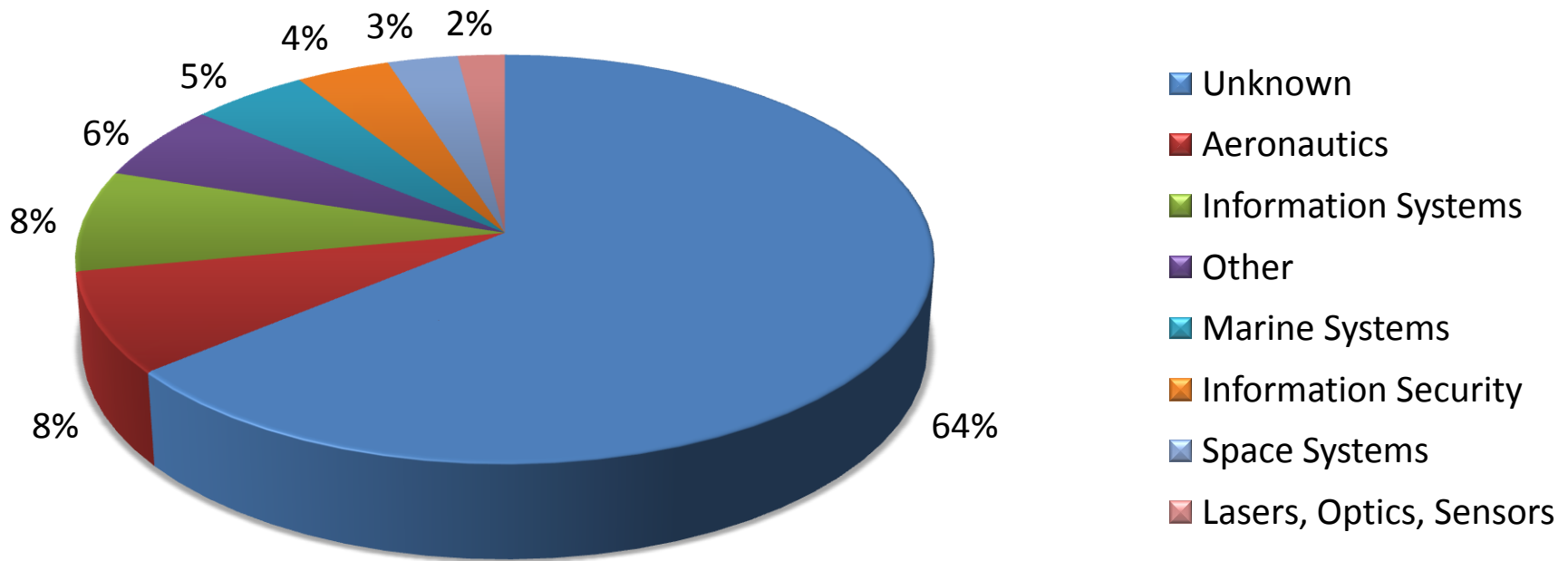
- (U//FOUO) 1,678 suspicious contact reports (SCR) categorized as cyber incidents (+102% from FY11)
- (U//FOUO) 1,322 of these were assessed as having a counterintelligence (CI) nexus or were of some positive intelligence (PI) value (+186% increase from FY11)
- (U//FOUO) 263 were categorized as successful intrusions (+78% increase from FY11)
- (U//FOUO) 82 SCRs resulted in an official investigation or operation by an action agency (+37% increase from FY11)

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) FY12 Technologies Targeted by Cyber

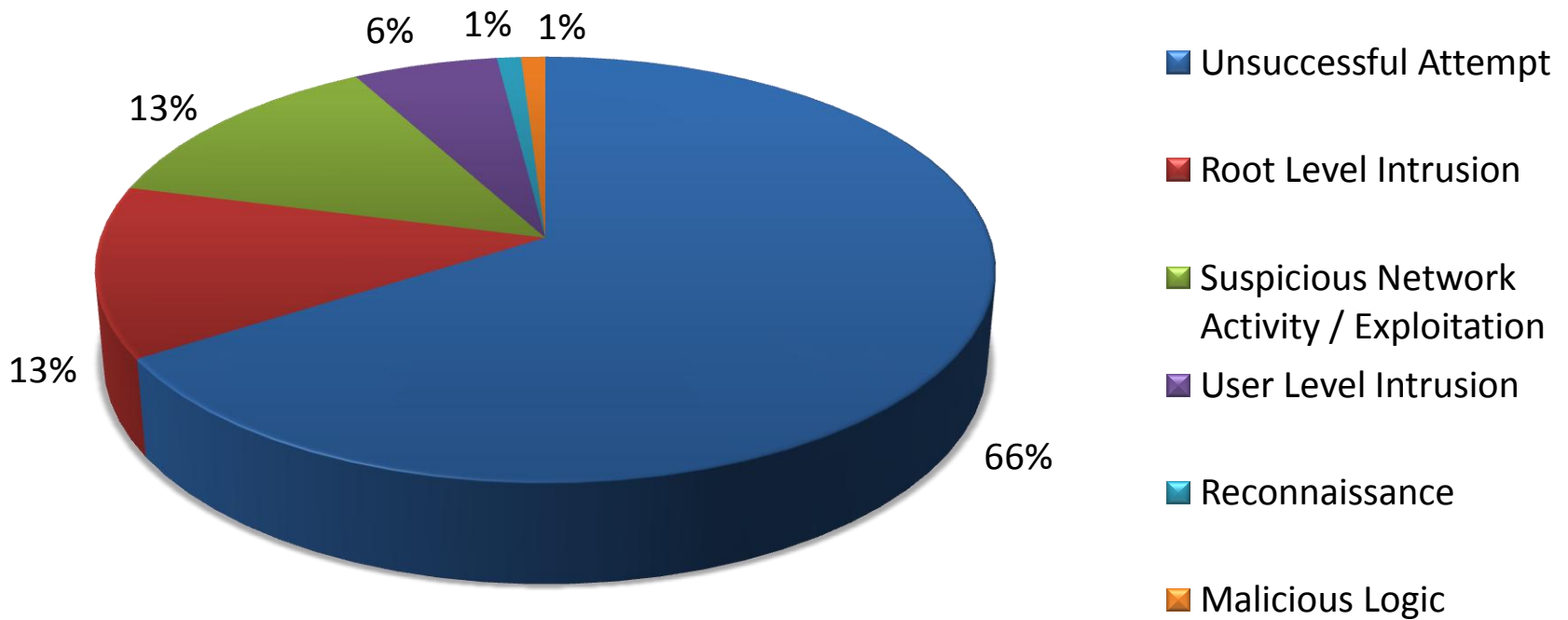


UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) FY12 Cyber Incident by Category



UNCLASSIFIED//FOUO



(U) Cyber Threats

- (U) Nation states (foreign governments)
- (U) Terrorist groups/extremists/sympathizers
- (U) Insiders
 - (U) Recruited
 - (U) Disgruntled Employee
- (U) Hackers/criminals
 - (U) Organized/individuals



ANONYMOUS

We are Legion. We do not Forgive. We do not Forget.



UNCLASSIFIED

(U) Where We Are Vulnerable

- (U) Bottom Line Up-Front: Everywhere
- (U) Application vulnerabilities (e.g., Internet Explorer, Adobe)
- (U) Operating systems
- (U) Web-based applications (e.g., JavaScript, Flash)
- (U) Removable media
- (U) Network-enabled devices
- (U) The end user



UNCLASSIFIED



UNCLASSIFIED

(U) Methods of Operation

- (U) Open source research
 - (U) Passive collection
- (U) Vulnerabilities and exploits
 - (U) Socially engineered email attacks
 - (U) 0-Day (Zero Day) application vulnerabilities
 - (U) Credentials
 - (U) Exploitation of trusted relationships (IT)
 - (U) Poor security practices/configurations
 - (U) Lack of end user education



UNCLASSIFIED



- (U) The model for handling threats **MUST** change
 - *“Conventional incident response methods fail to mitigate the risk posed by APTs because they make two flawed assumptions: response should happen after the point of compromise, and the compromise was the result of a fixable flaw”*
- (U) Intelligence-driven computer network defense is a necessity
 - (U) Address the threat component of risk, incorporating adversary analysis, their capabilities, objectives, doctrine and limitations



Threat Modeling

- (U) Intrusions must be studied from the adversary's perspective – analyzing the “kill chain” to inform actionable security intelligence
- (U) An adversary must progress successfully through each stage of the chain before it can achieve its desired objective



- (U) Just one mitigation disrupts the chain and the adversary






- (U) Moving detection and mitigation to earlier phases of the kill chain is essential in defending today's networks



UNCLASSIFIED//FOR OFFICIAL USE ONLY



DSS Counterintelligence Cyber Threat Advisory

Serial: DSS-TA-12-XXXX

(U//FOUO) Suspected Malicious Actors Change Spear Phishing Email Tactics, Techniques, and Procedures:

September 18, 2012

(U) Information cutoff date: September 18, 2012

(U) WARNING: THIS REPORT CONTAINS INFORMATION ON U.S. PERSONS. PROTECT IN ACCORDANCE WITH E.O. 12333. U.S. PERSON INFORMATION RETAINED UNDER DOD 5240.01 EXEMPTION 4.

(U) SUMMARY
(U//FOUO) This summary contains information derived from reports provided to the Defense Security Service (DSS).

(U//FOUO) On September 12, 2012, a California-based cleared contractor reported a computer network exploitation attempt by suspected malicious actors. Employees of the cleared contractor received a spear phishing email that appeared to come from the cleared contractor's chief financial officer (CFO). The actual email was sent from a webmail-based address. The email informed recipients of a salary increase due to excellent performance and provided a link to "access the salary."

(U//FOUO) The link in the email contained a condensed uniform resource locator (URL). Condensing a URL substantially shortens it while still directing the user to the intended page.¹

(U) FINDINGS
(U//FOUO) The following is the email received at the cleared contractor facility (reproduced exactly as seen by the recipient, with all grammatical errors):

From: USPER (CC CFO) [mailto:USPER@gmail.com]
Sent: Wednesday, September 12, 2012 7:36 AM
To: REDACTED
Subject: Pay Raise

Dear,

UNCLASSIFIED//FOR OFFICIAL USE ONLY





UNCLASSIFIED//FOUO

Why Your Reporting Matters

- (U//FOUO) Reporting establishes and/or confirms Foreign Intelligence Entities activities throughout Industry
- (U//FOUO) Provides leads for investigations and operations
- (U//FOUO) Provides high quality information to the Intelligence Community
- (U//FOUO) Provides valuable information that aides the Intelligence Community in articulating the threat to the highest levels of the U.S. Government
- (U//FOUO) Stolen unclassified DoD/U.S. Government data aids the adversary: strategically, operationally, tactically, diplomatically, economically, research and development, etc., etc...



UNCLASSIFIED//FOUO



- (U) Your DSS Community - ISR, ISSP, FCIS
- (U) Community Partnerships
- (U) Analytical Products
 - (U) SCR Responses, Cyber Activity Bulletin, Cyber Threat Advisories, Cyber Special Assessments, Crimson Shield, Scarlet Sentinel, Annual Cyber Trends
- (U) Homeland Security Information Network (HSIN)
- (U) DSS Cyber Security web-based training
 - <http://www.dss.mil/cdse/catalog/counterintelligence.html>
 - <http://cdsetrain.dtic.mil/cybersecurity>



BREAK



UNCLASSIFIED//FOUO

Defense Security Service

(U) Spear Phishing and Malware Submissions



UNCLASSIFIED//FOUO



UNCLASSIFIED
(U) Spear Phishing Sample #1

To: USPER

← Recipient Cleared Contractor

From: USPER@gmail.com

← Cleared Contractor Name Spoofed

Sent: Wednesday, September 12, 2012, 7:36 AM

Subject: Pay Raise

Malicious Hyperlink: Attempting to Entice Recipient to Click on Hyperlink by Adding Cleared Contractor Facility Name

Dear,

Given your recent excellent performance. We decided to increase your salary. Please access the Salary at the link below. Thank You.

Note: Adversary used the condensed URL to obfuscate the true malicious hyperlink

http://(US Cleared Contractor)/careers/Pay_Raise <http://goo.gl/J8y7P>

USPER
CFO
Email: USPER@gmail.com
Phone: Cleared Contractor Exact Number

← **Signature: Spoofed Cleared Contractor Name & Attempted to Use Exact Signature Block (Except Gmail Email Address Stood Out)**

- (U) When the condensed URL <http://goo.gl/J8y7P> is clicked, the user is redirected to the following link that hosts a suspected malicious file:
[https://thujfg\[.\]blu\[.\]livefilestore\[.\]com/y1p3n6liDN9rBDZQy6zRsRxERd8bWxlKKMp8rE0ZaRTjM98J8J7AfkxyLljWhvcy4XKxExwfAXcDmmT37Q_ALKdEw/Pay_Raise.zip?download&psid=1.2](https://thujfg[.]blu[.]livefilestore[.]com/y1p3n6liDN9rBDZQy6zRsRxERd8bWxlKKMp8rE0ZaRTjM98J8J7AfkxyLljWhvcy4XKxExwfAXcDmmT37Q_ALKdEw/Pay_Raise.zip?download&psid=1.2)
- Threat Advisory TA 12-020 was created on this incident (Found on HSIN Portal)



UNCLASSIFIED
(U) Spear Phishing Sample #2

To: USPER ← **Recipient Cleared Contractor**
From: Danny.Cho@email.com ← **Originating Email Address**
Sent: Tuesday, October 15, 2012
Subject: The New Strategic Pricing Capability

All,

attached is an advance copy of the PowerPoint slides for The New Strategic Pricing Capability.

Note: Punctuation Errors ←

Thanks

Danny

- **Included a Malicious Attachment “The New Strategic Pricing Capability.ppt**
- When PPT is opened, system is compromised and beacons to the following malicious URL:
Hxxp://www.video.onmypc.org
- The email header provided the originating email address which had been linked to nation state actors
- Details of Incident were provided in DSS’s Cyber Activity Bulletin 9 Nov 2012



UNCLASSIFIED
(U) Spear Phishing Sample #3

To: USPER ←

Recipient Cleared Contractor

From: Aimm <siraiya128@gmail.com> ←

Originating Email Address

Sent: Sunday, October 30, 2012

Subject: REQUEST FOR VISIT

Body of Email:

Password: 1qaz@WSX
please refer to the attached document for details ←

Note: Punctuation Errors & Email is
Not Addressed to the Individual

Regards,

Aimee

- **Included a Malicious Attachment “Visit_Plan.7z”**
- When zipped file is opened, system compromised and beacons to two command and control domains:
C2 #1: chroot[.]epac[.]to
C2#2: twcert[.]compress[.]to
- The C2 Domains have been linked to nation state actors
- Details of Incident were provided in DSS’s Cyber Activity Bulletin 26 Oct 2012



(U) Malware Submission Website - AMRDEC

UNCLASSIFIED

AMRDEC SAFE - Safe Access File Exchange - Windows Internet Explorer provided by Defense Security Service

https://safe.amrdec.army.mil/SAFE2/Default.aspx

File Edit View Favorites Tools Help

AMRDEC SAFE - Safe Acce... AMRDEC SAFE - Status AMRDEC SAFE - Safe A...

Home Help Support

Security Notice Accessibility Notice iSalute

UNCLASSIFIED USE ONLY, TO INCLUDE PRIVACY DATA

Personal Information

Your Name: [HELP](#)

Your Email Address: [HELP](#)

Confirm Your Email Address: [HELP](#)

File Information

Description of File(s):

Files: [Browse...](#) [HELP](#)

25 Maximum Files (total size cannot exceed 2GB)

File(s):

Deletion Date: *max is 14 days from today* [HELP](#)

Recipient Information

Provide an email address to give access to:

Manually Enter Email Address





(U) Malware Submission Website- AMRDEC

Recipient Information

Provide an email address to give access to:

Manually Enter Email Address

Email Address: [HELP](#)

Grant access to these people:

[HELP](#)

Email Setting

Caveats

NONE FOUO

Other:

Encrypt email message when possible [HELP](#)

Notify me when files are downloaded [HELP](#)

Require CAC for Pick-up (all recipients will need to log in with a CAC to download files) [HELP](#)

File Submission





UNCLASSIFIED//FOUO

(U) AMRDEC Safe Usage Policy Agreement

AMRDEC SAFE - Safe Access File Exchange - Windows Internet Explorer provided by Defense Security Service

https://safe.amrdec.army.mil/SAFE2/Default.aspx

File Edit View Favorites Tools Help

Files:

25 Maximum Files (total size cannot exceed 2GB)

File(s): C:\Users\jon.stevenson\Desktop\test.docx Privacy Act Data

Deletion Date: 08/15/2012 *max is 14 days from today*

Recipient Information

Provide an email address to give access to:

Manually Enter Email Address

Email Address:

Grant access to these people:

jon.stevenson@dss.mil

Email Setting

Caveats

NONE FOUO

Other:

Encrypt email message when possible

Notify me when files are downloaded

Require CAC for Pick-up (all recipients will need to log in with a CAC to download files)

File Submission

SAFE Usage Policy

I understand that the SAFE application is intended for official AMRDEC uses only and that it is NOT to be used for transferring personal files or any classified material.

I further understand that this is a Department of Defense interest computer system. All DoD interest computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems, including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. If monitoring of this or any other DoD interest computer system reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user may be provided to law enforcement officials.

Use of this computer system constitutes a consent to monitoring at all times. If monitoring reveals possible criminal activities or violations of security regulations, appropriate disciplinary action will be taken.

UNCLASSIFIED USE ONLY, TO INCLUDE PRIVACY DATA

Trusted sites | Protected Mode: Off

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) Verify Email Address

AMRDEC SAFE - Safe Access File Exchange - Windows Internet Explorer provided by Defense Security Service

https://safe.amrdec.army.mil/SAFE2/Default.aspx

File Edit View Favorites Tools Help

AMRDEC SAFE - Safe Access File Exchange

SAFE
Safe Access File Exchange

Home Help Support Security Notice Accessibility Notice iSalute

IMPORTANT: Your files cannot be downloaded by recipients until you verify your email address. Please check your email for further instructions.

The files were successfully uploaded.

You will receive a confirmation email shortly

Information on The Uploaded File(s)

File Name	File Size
[redacted].doc	27 KB
Total file size: 27 KB	

SAFE

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) Malware – Link to Verify Email Address

From: WEBTeam@amrdec.army.mil [mailto:WEBTeam@amrdec.army.mil]
Sent: Wednesday, October 24, 2012 2:27 PM
To: Recipient
Subject: VERIFICATION IS REQUIRED - AMRDEC Safe Access File Exchange Submittal Notice - VERIFICATION IS REQUIRED
Importance: High

DO NOT FORWARD

Please note, IAW Para 4-5.a(8) and 4-12.c, AR 25-2, it is a violation of SAFE security policy to share/forward Package passwords.

You must contact the Package originator to have the Package re-sent via SAFE (<https://safe.amrdec.army.mil/safe2/>) to other users.

Your Package has not yet been sent.

You MUST verify your email address in order for your recipients to download the file(s). Please use the link below to login and verify that you are the sender of this package.

<https://safe.amrdec.army.mil/safe2/StatusLogIn.aspx?PackageID=835595> (AMRDEC SAFE) ←

Click Link to Verify Email Address

If you did not send these files, please notify WebTeam@amrdec.army.mil ASAP.

You have uploaded the following file(s): This is a test file for Christina by Christina

Package ID: 835595

The file will be available until 11/7/2012

You can check the status of the files uploaded at <https://safe.amrdec.army.mil/safe2/StatusLogIn.aspx?PackageID=835595> (AMRDEC SAFE)

The Password is: 3GyB?7t#?wNd5v* ←

Password Needed

NOTICE: This e-mail message is intended solely for the use of the addressee. If the reader of this message is not the intended recipient, you are hereby notified that any reading, dissemination, distribution, copying, or other use of this message or its attachments is strictly prohibited. If you have received this message in error, please notify the sender immediately.

Thank you. ***This message may be forwarded to webteam@amrdec.army.mil for technical support purposes.***

UNCLASSIFIED//FOUO



(U) Malware – Verify Email to Submit File

1

AMRDEC SAFE - Check Status - Windows Internet Explorer provided by Defense Security Service
https://safe.amrdec.army.mil/safe2/Status.LogIn.aspx?PackageID=679357

File Edit View Favorites Tools Help

AMRDEC SAFE - Check Status

SAFE
Safe Access File Exchange

Home Help Support Security Notice Accessibility Notice iSalute

Note: This page is only for checking the package status. You cannot download files from this page.

To check the status of your package, enter your password:

2

AMRDEC SAFE - Status - Windows Internet Explorer provided by Defense Security Service
https://safe.amrdec.army.mil/safe2/Status.aspx?ID=679357

File Edit View Favorites Tools Help

AMRDEC SAFE - Check Sta... AMRDEC SAFE - Status

SAFE
Safe Access File Exchange

Home Help Support Security Notice Accessibility Notice iSalute

This package has not yet been sent. You must verify your email address by clicking the button below.

3

AMRDEC SAFE - Status - Windows Internet Explorer provided by Defense Security Service
https://safe.amrdec.army.mil/safe2/Status.aspx?ID=679357

File Edit View Favorites Tools Help

AMRDEC SAFE - Check Sta... AMRDEC SAFE - Status

SAFE
Safe Access File Exchange

Home Help Support Security Notice Accessibility Notice iSalute

Email address verified. The package has been sent.



(U) Malware – Submission Confirmation

AMRDEC SAFE - Status - Windows Internet Explorer provided by Defense Security Service

https://safe.amrdec.army.mil/safe2/Status.aspx?ID=679357

File Edit View Favorites Tools Help

AMRDEC **SAFE**
Safe Access File Exchange

Home Help Support Security Notice Accessibility Notice iSalute

Package ID: 679357
 Sender's Name: [Redacted]
 Sender's Email: [Redacted]
 Date Uploaded: 8/1/2012 10:53:02 AM
 Description: test
 Delete Date: 8/15/2012

File(s)	Privacy Act Data
[Redacted].doc (27 KB)	No

Upload more files to Package ...

New Recipient:

Resend Delivery Notice To:

Recipients	Downloaded
[Redacted]	False

The diagram illustrates the SAFE (Safe Access File Exchange) process. It shows two laptops, each with a padlock icon on its screen, representing secure endpoints. A large double-headed arrow connects the two laptops, with the word "SAFE" written in the center of the arrow, indicating the secure exchange of files between the devices.

Done Trusted sites | Protected Mode: Off 100%



UNCLASSIFIED//FOUO

Questions?

Jon Stevenson
jon.stevenson@dss.mil



UNCLASSIFIED//FOUO



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu