




Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

SECURITY SERVICE
UNITED STATES OF AMERICA

Cyber Enabled Threats to Cleared Industry



Cyber Enabled Threats to Cleared Industry

CDSE

Host: Rebecca Morgan –
Counterintelligence Instructor CDSE

Guest: Jeffrey Burlette –
DSS Counterintelligence Directorate

Producer: Sandy Vega – CDSE



Navigation in the Meeting Room

CDSE

Enlarge Screen

File Share



Closed Captioning below

Q & A


Center for Development of Security Excellence
CDSE
Learn. Perform. Protect.





Cyber Enabled Threats to Cleared Industry

 **Agenda** 

- Counterintelligence, Cyber Counterintelligence, and the NISP
- The DSS Mission and Counterintelligence Role
- Cyber Enabled Intelligence Activities
- Reporting Requirements

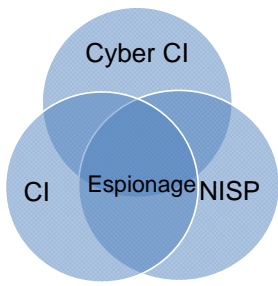


 **Cyber Enabled Threats to Cleared Industry** 



What is Counterintelligence?

What is Cyber Counterintelligence?

How do these definitions apply to the NISP?



6

	Cyber Enabled Threats to Cleared Industry	
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 U.S. Government leaders.		
Scope - 10+K firms, 13+K facilities, 1.2m people - 1 CI professional/261 facilities - 12% of facilities report		

	Cyber Enabled Threats to Cleared Industry							
How does Cyber enable intelligence activities at cleared industry?								
<table border="1"> <tr> <th style="text-align: center;">Academic Solicitation</th> </tr> <tr> <td> <ul style="list-style-type: none"> Typically a foreign student contacts a professor Builds a trust through communicating via email Trust relationship is exploited by sending a weaponized academic paper to the target </td> </tr> </table>	Academic Solicitation	<ul style="list-style-type: none"> Typically a foreign student contacts a professor Builds a trust through communicating via email Trust relationship is exploited by sending a weaponized academic paper to the target 	<table border="1"> <tr> <th style="text-align: center;">Seeking Employment</th> </tr> <tr> <td> <ul style="list-style-type: none"> Foreign actor seeking employment with a cleared company Easily send a weaponized resume to the unsuspecting employer </td> </tr> </table>	Seeking Employment	<ul style="list-style-type: none"> Foreign actor seeking employment with a cleared company Easily send a weaponized resume to the unsuspecting employer 	<table border="1"> <tr> <th style="text-align: center;">Exploitation of Relationships</th> </tr> <tr> <td> <ul style="list-style-type: none"> Exploit the relationship to entice an employee to open a malicious email Can leverage trust to insert removable media into a company computer </td> </tr> </table>	Exploitation of Relationships	<ul style="list-style-type: none"> Exploit the relationship to entice an employee to open a malicious email Can leverage trust to insert removable media into a company computer
Academic Solicitation								
<ul style="list-style-type: none"> Typically a foreign student contacts a professor Builds a trust through communicating via email Trust relationship is exploited by sending a weaponized academic paper to the target 								
Seeking Employment								
<ul style="list-style-type: none"> Foreign actor seeking employment with a cleared company Easily send a weaponized resume to the unsuspecting employer 								
Exploitation of Relationships								
<ul style="list-style-type: none"> Exploit the relationship to entice an employee to open a malicious email Can leverage trust to insert removable media into a company computer 								
								

	Cyber Enabled Threats to Cleared Industry				
How does Cyber enable intelligence activities at cleared industry?					
<table border="1"> <tr> <th style="text-align: center;">Attempted Acquisition</th> </tr> <tr> <td> <ul style="list-style-type: none"> Front company attempting to acquire controlled technology Can hide true identity and intentions by communicating electronically </td> </tr> </table>	Attempted Acquisition	<ul style="list-style-type: none"> Front company attempting to acquire controlled technology Can hide true identity and intentions by communicating electronically 	<table border="1"> <tr> <th style="text-align: center;">Request for Information</th> </tr> <tr> <td> <ul style="list-style-type: none"> Usually request is sent over email Typically involves multiple email exchanges between actor and company Actor can easily send weaponized document during one of the exchanges </td> </tr> </table>	Request for Information	<ul style="list-style-type: none"> Usually request is sent over email Typically involves multiple email exchanges between actor and company Actor can easily send weaponized document during one of the exchanges
Attempted Acquisition					
<ul style="list-style-type: none"> Front company attempting to acquire controlled technology Can hide true identity and intentions by communicating electronically 					
Request for Information					
<ul style="list-style-type: none"> Usually request is sent over email Typically involves multiple email exchanges between actor and company Actor can easily send weaponized document during one of the exchanges 					
					

Cyber Enabled Threats to Cleared Industry CDSE

How does Cyber enable intelligence activities at cleared industry?

Foreign Visits <ul style="list-style-type: none">• Can overtly/covertly insert malicious removable media into a company computer 	Potential Espionage Indicators <ul style="list-style-type: none">• An Insider can use cyber means to elevate access on the network, easily gain access to files, and place malware on the network for foreign actors to leverage. 
---	--

Cyber Enabled Threats to Cleared Industry CDSE

How does Cyber enable intelligence activities at cleared industry?

Suspicious Network Activity


- Spear phishing
- Compromised credentials
- Website compromise
- Social Networking Sites
- SQL injection



Cyber Enabled Threats to Cleared Industry CDSE

How Does the Company Protect Itself?

- Maintain good network hygiene!
- Implement good firewall rules
- Block file extensions at the email gateway
 - EXE, SCR, ZIP, VBS, etc.
- Block dynamic DNS domains
- Assume you will be compromised at some point
 - Shorten your mean time to know




Cyber Enabled Threats to Cleared Industry


How Does DSS Help?

- Defensive Cyber Operations
 - Threat products
 - Advise and assist
- Offensive Cyber Operations
 - Contractor Suspicious Contact Report referrals
- Strategic Analysis
 - Threat = Capability x Opportunities x Intent
 - Used to anticipate adversary operations




Cyber Enabled Threats to Cleared Industry


Suspicious Contact Reporting:

- NISPOM 1-302b
- NISPOM 1-301




Cyber Enabled Threats to Cleared Industry


Counterintelligence Training Products

Related Training

- Protecting Your Facility's Technology
- Cybersecurity Awareness
- Suspicious Emails

Job Aids

- Counterintelligence Awareness Toolkit

Past Webinars

- Cyber Insider Threat
- Information Security Continuous Monitoring
- Reportable Unclassified Cyber Events


www.cdse.edu/catalog/counterintelligence.html



 **Cyber Enabled Threats to Cleared Industry** **CDSE**

Question and Answer Session 




 **Cyber Enabled Threats to Cleared Industry** **CDSE**


Feedback

Before we conclude today's presentation, we hope you'll take a moment to participate in our feedback questionnaire. Your feedback is very helpful to us and is greatly appreciated.

If you have ideas for future webinar topics, you can share these in the questionnaire.

 **Cyber Enabled Threats to Cleared Industry** **CDSE**

Counterintelligence Training POC:



Peter DeCesare and Rebecca Morgan
(410) 689-1136 (410) 689-1294
Email: counterintelligence.training@dss.mil
