Welcome and Opening Remarks from FISSEA Co-Chair

Maureen Premo
FISSEA Co-Chair
Immigration and Customs Enforcement
Department of Homeland Security
Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUUpdates@list.nist.gov

Volunteer for the Planning Committee

Serve on the Contest or Award Committees for 2022
Email fissea@nist.gov

#FISSEA
OPEN year-round

March 18, 2022 – deadline for FISSEA Spring Forum priority consideration

Submit proposals at:
https://www.surveymonkey.com/r/fisseacallforpresentations
FISSEA Innovator of the Year Award

Recognize an individual who has made significant contributions in inspiring the strategic planning, building, and management of innovative cybersecurity awareness and training programs.

Nominations due April 4, 2022

Submit nominations at: https://www.surveymonkey.com/r/fisseainnovatorform

#FISSEA
Best Practices for Diversity and Inclusion in Training

Diann W. McCants, Ph.D.
Strategic Analysis, Inc.
Contractor Support to Laboratories and Personnel
Office of the Under Secretary of Defense for Research and Engineering
Best Practices for Diversity and Inclusion in STEM:
A Guide by and for Federal Agencies

A REPORT BY THE INTERAGENCY WORKING GROUP ON INCLUSION IN STEM

DR. DIANN W. MCCANTS
LABORATORIES AND PERSONNEL OFFICE, DOD (CONTRACTOR SUPPORT)
Overview

• The IWGIS was established according to the American Innovation and Competitiveness Act (2017)
• An interagency working group under the Committee on STEM Education (CoSTEM) and the Federal Coordination in STEM Education (FC-STEM) Subcommittee
• Collaborative effort of representatives from 19 Federal agencies
• Why this document now
  • Executing a strategic approach
  • Critical role of diversity, equity, inclusion and accessibility: Priority of current Administration
    • Executive Order 14035: Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce
• The process for developing this summary of best practices that can be employed by Federal agencies as they implement strategies to promote diversity and inclusion in the Federal STEM workforce included:
  • Developing definitions
  • Reviewing the literature
  • Soliciting best practices from Federal agencies
Overview of CoSTEM

*Congressionally Mandated
### Key Contributors

#### Report Writing Team

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. Maria Carranza</td>
<td>HHS/NIH</td>
</tr>
<tr>
<td>Dr. Amy D’Amico</td>
<td>SI</td>
</tr>
<tr>
<td>Ms. Tajjay Gordon</td>
<td>NSF</td>
</tr>
<tr>
<td>Mr. Noller Herbert</td>
<td>USDA</td>
</tr>
<tr>
<td>Dr. Sylvia Butterfield</td>
<td>NSF</td>
</tr>
<tr>
<td>Dr. Charlene Le Fauve</td>
<td>HHS/NIH</td>
</tr>
<tr>
<td>Ms. Yuliya Manyakina</td>
<td>NSF</td>
</tr>
<tr>
<td>Dr. Diann McCants</td>
<td>DOD</td>
</tr>
<tr>
<td>Dr. Eleanour Snow</td>
<td>DOI/USGS</td>
</tr>
<tr>
<td>Dr. Natasha White</td>
<td>NOAA</td>
</tr>
</tbody>
</table>

#### Other Key Contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ms. Grace Hu</td>
<td>OMB</td>
</tr>
<tr>
<td>Dr. Marlene Kaplan</td>
<td>DOC/NOAA</td>
</tr>
<tr>
<td>Mr. Greg Simmons</td>
<td>DHS</td>
</tr>
<tr>
<td>Ms. Dawn Tucker-Thomas</td>
<td>DOT</td>
</tr>
<tr>
<td>Dr. Julie Carruthers</td>
<td>DOE</td>
</tr>
<tr>
<td>Ms. Leslie Wheelock</td>
<td>FDA</td>
</tr>
<tr>
<td>Mr. Bryant Maldonado</td>
<td>HHS/NIH</td>
</tr>
<tr>
<td>Dr. Dane Samilo</td>
<td>DOD</td>
</tr>
</tbody>
</table>
Key Topics Covered

• Definitions
• Current Status of the Federal STEM Workforce
• Barriers to Diversity and Inclusion in STEM
• Key Areas for Advancing Diversity and Inclusion in STEM
• Promising and Emerging Practices
• Recommendations to Help Increase Recruitment, Retention, Achievement, and Advancement of Underrepresented Groups
Introduction

• Understanding and identifying barriers within Federal agencies and STEM pathways is integral to developing and implementing best practices.

• This content was assembled from an extensive STEM literature review.

• It provides an overview of leading institutional and individual barriers to diversity and inclusion in STEM.
Barriers to Diversity and Inclusion

Barriers Cover Numerous Areas

- Policies
- Workplace Climate
- Differential Compensation Packages
- Availability and Use of Data
- Cost of Education
- Workplace Interactions
- Individualized STEM Workforce Barriers

- Perceptions of STEM Programs
- Stereotypes and Stereotype Threat
- Biases
- Science Identity
- Accessibility for Individuals with Disabilities
Key Areas for Advancing Diversity and Inclusion in STEM

- STEM Pathways
- Access and Recruitment
- Achievement and Advancement
- Retention

INTERAGENCY WORKING GROUP ON INCLUSION IN STEM
Key Areas for Advancing Diversity and Inclusion in STEM

Example

The NASA Community College Aerospace Scholars (NCAS) is a nationwide activity designed for post-traditional learners enrolled in an accredited 2-year institution in the U.S. who are interested in a STEM career.

- Helps students make the connection between a STEM degree and NASA career opportunities
- Prepares and motivates students to participate in other competitive NASA projects, programs, and internships
- Encourages community college students to finish their 2-year degree and pursue a 4-year degree or career in a STEM field
Key Areas for Advancing Diversity and Inclusion in STEM

Access and Recruitment

Broad access and Intentional Recruitment are Critical

Partnerships in support of individuals from groups currently underrepresented in STEM

Leverage Human Resources Departments

Human Resources Departments can play a key role:

- Identify and change recruitment and hiring practices that fail to be inclusive
  - Consider marketing materials, recruitment sources, qualifying questions and candidate scoring rubrics, make-up of hiring committees, and the interview processes
- Address unconscious bias. For example, rather than viewing hiring persons with disabilities as just being “the right thing to do,” it must be viewed as part of a talent strategy that will benefit the organization
- Use appropriate data for comparison when assessing diversity and inclusion internal to your agency
  - For example, only 13% of companies in the U.S. have reached the Department of Labor’s target of having 7% disability representation in their workforce
Key Areas for Advancing Diversity and Inclusion in STEM

Retention

Retention is key in maintaining D&I
Alignment of institutional culture and climate
Institutional Commitment and Accountability
Data Disaggregation and Intersectionality

Data Disaggregation and Intersectionality:
To adequately understand the issues that impact retention, institutions must look at differences by population and STEM discipline as an important factor in implementing effective strategies for change

• Data disaggregated by populations, geographical regions, and race/ethnicities is critical to STEM participation, identifying target populations, and capturing their unique characteristics
• Furthermore, data must be disaggregated by sex within race/ethnicity, disability, citizenship, and STEM discipline to understand the experiences at the intersection of different identities
• Evaluation studies with disaggregated data can help leaders set goals related to their duties and responsibilities and be more reflective about their decision-making processes
Achievement and Advancement

Achievement can be related to individuals, but the opportunity for achievement is systemic

Establish clear guidelines for evaluation and promotion

Develop robust systems of support

Create opportunities and pathways for growth

Example

The NIST International and Academic Affairs Office (IAAO) implements several best practices to support inclusion in STEM through achievement and advancement, as well as retention

• IAAO utilizes affinity groups and employee resource groups to raise awareness and expand networks for diversity and inclusion in STEM

• The mission of the Steering Group for Equity in Career Advancement is to identify the causes of apparent inequities in promotions at NIST for women and minority researchers and make recommendations
Recommendations

• Recommendations are grouped into four categories to address:
  • Use of definitions for evidence-based, emerging, and promising practices
  • Barriers to participation in STEM
  • Ways to increase diversity and inclusion in STEM
  • Incorporating emerging and promising practices
To Use Definitions

• Use the definitions of evidence-based, emerging, and promising practices to explain the best practices that are used

• These definitions will:
  • Clarify what works and why a practice is adopted for a specific group
  • Substantiate the expectations of effectiveness
To Address Barriers to Participation

• Identify barriers to access and participation in STEM programs and partner with other agencies, institutions, and professional organizations

• Create a comprehensive plan that includes incentives for participants and grantees to demonstrate progress.
To Address Barriers to Participation

- Focus on one or more **institutional** barriers to STEM such as policies, workplace climate, differential compensation packages, data, and peer-to-peer interactions.

- Require program participants and grant recipients to share how they will reduce or eliminate institutional barriers to diversity in STEM.
To Address Barriers to Participation

• Focus on one or more **individualized** barriers to participation in STEM and develop programs that address areas such as mentoring, support systems, discrimination, perception of STEM programs, stereotypes and stereotype threat, bias, and STEM identity

• Focus on one or more barrier impacting STEM participation for individuals with disabilities
  • Develop policies and practices to ensure their representation in leadership and decision-making bodies
Recommendations

To Increase Diversity and Inclusion

• Develop a pathways approach to STEM academic and career programs that allows multiple entry points allowing participants to build on their academic achievement and research expertise

• Identify barriers to access and participation in STEM programs then develop strategies to reduce or eliminate them by partnering with other agencies, institutions, and professional organizations
To Increase Diversity and Inclusion

• Create a plan and provide opportunities for leadership training and skills development
• Use existing Federal leadership programs or create leadership development efforts
• Provide unconscious bias training for existing managers to raise awareness about the impact of implicit bias
To Increase Diversity and Inclusion

• Use existing hiring authorities to diversify the Federal STEM workforce at all levels

• Develop more flexible hiring pay authorities, particularly for entry level positions

• Create authority for Federal scholars and fellows to be hired noncompetitively into Federal service
Questions

Thank You!

Susan Hansche
FISSEA Chair
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security
Standards and Guidance for Cybersecurity Training Program: Updates to NIST Special Publications 800-50 and 800-16 Creating a Cybersecurity and Privacy Awareness and Training Program

Marian Merritt
Deputy Director
National Initiative for Cybersecurity Education (NICE)
National Institute of Standards and Technology

Jess Dickson
IT Specialist (Privacy)
Privacy Engineering Program
National Institute of Standards and Technology

#FISSEA
Update to NIST SP 800-50/800-16
Marian Merritt and Jess Dickson
Outline

• Overview of the project
  – History of the publications
  – Why update now?

• Key Objectives

• Work to Date

• Take-aways from pre-draft comments

• Next steps

• Q&A
Overview: History of the publications:

• 800-50: “Building an Information Technology Security Awareness and Training Program”
  – October 2003
  – Foundational document to guide creation of an organization’s cybersecurity A/T program
Overview: History of the publications (cont):

- **800-16 “Information Technology Security Training Requirements: A Role and Performance-Based Model”**
- April 1998
- Revised:
  - V1 3rd draft 2014
  - Prelim draft R2 2020 (not published)
Overview: Why Update Now?

• Opportunity to sync NIST guidance with latest updates and recommendations from outside guidance informing this work
  – OMB A-130
  – National Defense Authorization Act (NDAA) for FY2021
  – Cybersecurity Enhancement Act of 2014

• Opportunity to address gaps and open questions within existing guidance
Key Objectives

- Update to security awareness and training program lifecycle
- Incorporating privacy awareness and training programs in parallel with security
- Consolidation of 800-50 and 800-16
- Incorporate NICE Workforce Framework KSTs
Work to Date

• Co-authoring team formed:
  – NIST (NICE and Privacy Engineering), DHS, OPM, DOT

• Pre-draft Call for Comments
  – Issued Sept. 21, 2021
  – Closed Nov. 5, 2021
  – Adjudication completed Jan. 2022
Take-aways from pre-draft comments

• Interest in an iterative lifecycle approach
• Desire for flexibility, scalability
• Standardized, clearly defined terms
  – E.g., awareness, literacy training, role-based training
• Wider stakeholder and SME input
• Reflect current work environment and requirements (i.e. remote workforce)
Take-aways from pre-draft comments (cont)

• Importance of tying A&T programs together with security & privacy risk management efforts
• Metrics – what is useful, what can be measured
• Feedback mechanisms
• Post-implementation assessment steps
Today:

• Incorporating Julie Haney/Jody Jacobs research
  – Focus groups with Cybersecurity Training/Awareness Managers
• Finalizing outline
• Assigning sections to SMEs on authoring team
Next Steps: Rough Timeline

- February - Co-authors collaborate on a draft
- March - Internal review NIST and other agencies
- Late March – **publish for comments (45 days)**
- May – June: adjudicated comments/revise
- July – internal review
- August/September – final version
Questions?
Thank You!
Federal Information Security Educators (FISSEA) Fall Forum

BREAK

The Forum will resume at 2:45pm ET

#FISSEA | nist.gov/fissea
Welcome Back!

Susan Hansche
FISSEA Chair
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security
An Overview of SMS/Text Scams Impersonating State and Federal Agencies During the Pandemic

Mark Henderson
Online Fraud Detection and Prevention
Internal Revenue Service
An Overview of SMS/Text Scams Impersonating State and Federal Agencies During the Pandemic

Mark Henderson
Internal Revenue Service
Online Fraud Detection and Prevention
OS:CTO:C:O:OFDP
Desk: 202-556-2615
mark.w.henderson@irs.gov
Disclaimer

Any views or opinions are my own and do not necessarily reflect the official views of the U.S. Treasury.
What is SMS?

• Short Message Service (SMS)
• Message size is limited (160 characters)
• Supports multiple alphabets
• Makes use of “short codes”

• **A Lure**: enticing email content

• **A Hook**: an email-based exploit
  • Email with embedded malicious content that is executed as a side effect of opening the email
  • Email with malicious attachments that are activated as a side effect of opening an attachment
  • Email with “clickable” URLs: the body of the email includes a link, which displays as a recognized, legitimate website, though the actual URL redirects the user to malicious content

• **A Catch**: a transaction conducted by an actor following a successful attempt
  • Unexplainable charges
  • Unexplainable password changes
What is smishing?

• MMS/SMS/text + social engineering ("phishing") = "smishing"
• These text messages will typically contain a domain/URL
• This domain/URL will typically lead directly/indirectly to a phishing site ("landing page")
• In some cases, the text message will only include a telephone number that the recipient needs to "text", with no domain/URL to "click"
Why the uptick in SMS phishing?

- **Exploiting work-from-home (WFH)** - “It’s far easier to block email phishing on corporate-owned PCs, but today’s remote workers are now using their personal devices to access corporate apps and data.”

- **“fish in a barrel”** - “The devices are literally everywhere, providing a vast, exploitable threat landscape for hackers [2.8B devices worldwide].”

- **Higher click rates** - “Consider that 90 percent of text messages are opened and read almost immediately; meanwhile, the average open rate for email hovers around 20 percent.”

- **Lack of security protections** - “Personal devices typically lack the robust security used to protect corporate devices.”

- **Distraction** - “... we’re just not paying attention.”

Smishing requires different abuse handling

• Smartphones have limited screen real-estate
• SMS messages aren’t typically provided in their raw text form
• Typosquatting makes identifying the URL from a screenshot difficult
• SMS messages can be difficult to trace
Reporting smishing

• Reporting the text of the SMS/text is best: press on a blank area of the message and select “Copy”

• IRS-related smishing can be reported:
  • via SMS using 202-552-1226 and/or email to phishing@irs.gov (e.g., plain ASCII or screenshot)

• IRS-related and non-IRS smishing can also be reported:
  • via the messaging app
  • by copying the message and sending to 7726 (SPAM)
  • to the Federal Trade Commission (FTC) at ftc.gov/complaint
Caveat about 7726

- Forwarding to 7726 does **not** remove the actual phishing content
  - 7726 provides details of the message to the telecommunications provider
- Filing a complaint with the FTC typically does **not** action the phishing content
- You will need to report the numbers and the domains/URLs separately
“Joe Biden” Pandemic smish

• “406-559-0719” = Verizon
• “forms.zohopublic.com” is a free online form builder
• Potential “man in the mailbox” phishing attempt

hxxps://forms[.]zohopublic[.]com/pandemicrelief2/form/UNEMPLOYMENTINSURANCERELIEF/formperma/ZITMZ0x_p-rcri1UhmxmOVImMspoPKQVd3zAn6vRc8Y
“Joe Biden” Pandemic smish

• “Unemployment Insurance Relief”
• “Unemployment Insurance Application Form”

hxxps://forms[.]zohopublic[.]com/pandemicrelief2/form/UNEMPLOYMENTINSURANCE_RELIEF/formperma/ZITMZ0x_p-rcxi1UhmxmOVIImMspoPKQVd3zAn6vRc8Y
“Joe Biden” Pandemic phishing site (cont.)

- “Front of your State ID/License”
- “Back of your State ID/License”
- “Front of your SSN CARD”
- “Back of your SSN CARD”
smishing scams sent to phishing@irs.gov

- **phishing@irs.gov** receives a variety of online scams including smishing scams
- Smishing sent to **phishing@irs.gov** often references:
  - IRS, Treasury and/or is tax-related
  - USG programs (e.g., CARES Act)
  - One or more other USG agencies
  - State, Local, Tribal and Territorial (SLTT) (e.g., State Workforce Agencies)
  - None of the above (e.g., banks, telcos, etc.)
# of reported IRS-related smishing incidents

Current as of 2022-01-24
IR-2020-167: Press release

IRS warns people about a COVID-related text message scam

COVID Tax Tip 2020-167, December 8, 2020

The IRS and its Security Summit partners are warning people to be aware of a new text message scam. The thief’s goal is to trick people into revealing bank account information under the guise of receiving the $1,200 Economic Impact Payment.

Here's how this scam works

People get a text message saying they have "received a direct deposit of $1,200 from COVID-19 TREAS FUND. Further action is required to accept this payment..." The text includes a link to a phishing web address.
Smishing versus Vishing complaint volume

Current as of 2022-01-24
% of IRS smishing that is “stimulus”-themed

Current as of 2022-01-24
Examples of observed techniques

• AT&T Email to Text
• Fraudulent domains serving as a redirects
• Redirection leveraging trusted sites (i.e., legitimate URL shorteners redirecting to phishing URLs)
• “Numbers-only” smish (i.e., no URL or domain)
AT&T email-to-text

If you create an email with an AT&T telephone number as the username, you can send a text message from your email

“[1234567890]@txt.att.net”

1410100013
AT&T Smish - Fraudulent domain as redirect

• 1410100025 = AT&T email-to-text
• f2c[.]host is a fraudulent domain
• Domain redirected to a “Get My Payment” phishing site
• Phishing landing page asked for screenshot of the victim’s Driver’s License, front and back

hxkp://www[.]f2c[.]host/?IRS10471482128
“Chaining” multiple redirects is common

curl –vv ‘hxxp://www[.]f2c[.]host/?IRS10584232211’
...
HTTP/1.1 301 Moved Permanently
Location: hxxps://f2c[.]uno/redi/3? IRS10584232211’

f2c[.]{host,uno}
Registrar: Hostinger
Creation Date: 2021-02-26
Leveraging Trusted Sites (e.g., lnkd.in)

- 309-512-3852 = AT&T
- lnkd[.]in is a LinkedIn URL shortener
- See the Living off Trusted Sites Project (lots-project.com)
- Redirected to a website using dynamic DNS

hxxps://lnkd[.]in/euHT2Bg
"Get My Payment" phishing website

myaccount-gov[.]sytes[.]net/?access_protect
IRS EIP “numbers-only” smish

• 336-524-3275 = Verizon
• 920-341-5658 = Bandwidth
• No domain and/or URL in the message
• Small number of recipients
State, local, tribal and territorial (SLTT) agencies
Overview

• Fraudsters continue to send a variety of scams to taxpayers via email, text and social media
• During the pandemic, a subset of complaints we received were from individuals reporting scams targeting various state benefits programs
• Fraudsters are creating phishing websites (e.g., fake State unemployment web portals)
• Fraudsters are collecting victim information (e.g., email credentials, driver’s license, etc.)
• This information is then used to conduct different types of fraud (e.g., unemployment insurance fraud)
What States have (already) observed

- California (CA) - “DMV warning customers about a text message scam”
- Florida (FL) – “Text scammers have new ploy posing as the DMV”
- Illinois (IL) – “Illinois residents targeted by scam text messages” [“... scam text messages from the DMV”]
- New York (NY) – “New York State DMV warns of new text messaging scam”
- Texas (TX) - How to Spot the Latest Scam Texts, Emails Targeting Texans [“Texas Department of Motor Vehicles”]
Arkansas smishing lure

“Your Arkansas Unemployment Insurance Claim account is currently on hold for verification, Please complete your verification by following the instructions in the link below: hxxps://tinyurl[.]com/n5emccpf to reactivate your account.”

hxxps://tinyurl[.]com/n5emccpf
California smish

• 347-785-0194 = Verizon
• mybenefitclaims[.]com: Namecheap
• “Rita L. Saenz Director Employment Development”

hxxp://www[.]mybenefitclaims[.]com/
Illinois smish

• t[.]co = URL shortener (Twitter)  

Office secretary of state(IL):

DL Details seems to be missing or Incorrect.

Follow steps:hxxps://t[.]co/wMC1usiAwx

hxxps://t[.]co/wMC1usiAwx
Illinois smishing landing page

- Picture of “Jesse White”, IL Secretary of State
- “Driver’s License Number”
- “Social Security Number (000-00-000)”
- Contact Number

https://docs.google.com/forms/d/e/1FAIpQLSe88iCqdgV0FW5PYB03NQRqjC4lq7-WOb-1AVff48kwU3ow0g/viewform
Maryland smish

- 833-851-0738 = Vonage
- “beacon.labor.maryland.gov” is the sub-domain but not the actual domain
- labor-maryland[.]com = Tucows
Maryland smishing landing page

hxxps://beacon.labor.labor.maryland.gov.labor-maryland[.]com/
Resources

- CISA ("Avoiding Social Engineering and Phishing Attacks")
- FCC ("Consumer Tips to Stop Unwanted Robocalls and Avoid Phone Scams")
- FCC ("FCC Smartphone Security Checker")
- FTC ("How To Recognize and Report Spam Text Messages")
- IRS ("Here's How To Avoid IRS Text Message Scams")
What can your organization do about it?

- Recognize fraudulent components of common scams (e.g., domains, emails, URLs, numbers, social media profiles/sites, etc.)
- Establish workflows to record/report abuse to the appropriate service providers
- Provide an email alias and/or online form to report scams to your organization
- Provide victims with additional resources for reporting (e.g., IC3.gov) on your website and/or in your auto-reply
- Identify victim information if possible and then share with appropriate groups
- Share lessons learned with others
Questions?

mark.w.henderson@irs.gov
Showcasing the Use of a Cyber Range for the President's Cup Competition

Michael Harpin
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

#FISSEA
President’s Cup Cybersecurity Competition

Building a Competition Across the Federal Workforce
### What is the President’s Cup Cybersecurity Competition?

- America’s Cybersecurity Workforce E.O. 13870 mandates DHS to hold the competition annually.

- The goal of the competition is to identify and reward the top cybersecurity talent in the federal workforce.

- Any federal executive department or agency employee can participate, including uniformed service members.

- Participants can compete as an Individual, on a Team of up to five members, or both.

#### 2021 Winners

<table>
<thead>
<tr>
<th>Individual Track A</th>
<th>Individual Track B</th>
<th>Team 780th Military Intelligence Brigade</th>
</tr>
</thead>
<tbody>
<tr>
<td>USMC</td>
<td>USAF</td>
<td>780th Military Intelligence Brigade</td>
</tr>
</tbody>
</table>

86
Considerations for President’s Cup Platform

- Accessible anywhere from a standard web browser
  - Minimum Hardware/Software requirements for end users
- Scalable to support potentially thousands of concurrent participants across the federal .gov/.mil
- Open-Source Resources
  - TopoMojo – [https://github.com/cmu-sei/TopoMojo](https://github.com/cmu-sei/TopoMojo)
  - Gameboard - [https://github.com/cmu-sei/Gameboard](https://github.com/cmu-sei/Gameboard)
  - Identity - [https://github.com/cmu-sei/Identity](https://github.com/cmu-sei/Identity)
President’s Cup Challenge Development

- Each challenge is tied to a NICE Work Role
- Built within TopoMojo
  - Multiple variants of each challenge created and deployed at random
  - “Infinity challenges” – variants within challenge randomized by TopoMojo
- Quality Assurance for each challenge
  - Playtesting conducted by National Labs with support of DOE
- Session timer
  - Influences challenge development and competitor strategy
Accessing the Challenges

Status

Date: 19th February 2022

Background

Analyze This!

1. What is the goal of the game?
2. What are the obstacles in the game?
3. What is the objective of the player?

Getting Started

Submit your answers online to the game's website.

Challenge Questions

1. Which level requires the most strategy?
2. Which level offers the least challenge?
3. Which level requires the most patience?

System Credentials

Username: [username]
Password: [password]

Gameplay Resources

- [Link 1]
- [Link 2]
Gameboard Updates in 2021

- Consolidated Gameboards into a single application
- Integrated challenge metadata
- Migrated email functionality away from Gameboard
  - PII protections
Foundry Appliance

- Pre-configured VM that packages President’s Cup applications
- Single-host Kubernetes cluster to replicate production deployment
- Uses VMware ESXi to serve virtual challenge environments
- https://github.com/cmu-sei/foundry-appliance
Outlook for President’s Cup System

- Moving system to DHS cloud environment.
  - Potential for additional competitions and challenge developers.
- Standing up archive site.
- Releasing source code of challenges to public after each competition.
- Continued development of Foundry Appliance
President’s Cup Format

- The competition has three rounds – two Qualifying Rounds and Finals.
- Qualifying Rounds
  - Must succeed in first qualifying round to participate in second round
    - Teams – best team from each Department, plus top 20% based on score
    - Individuals – Top 100
- Final Round
  - Top 5 Teams and Top 10 Individuals in Tracks A/B
  - Day 2 of Teams Finals Livestreamed via YouTube
Insider Threat Program Training: Gaining Management Awareness and Support

Rebekah Ibarra
Insider Threat Program Manager
Social Security Administration

Joe Hoofnagle
Senior Advisor Cybersecurity & Intelligence
Social Security Administration

#FISSEA
Insider Threat Program Training

Gaining Management Awareness and Support

February 15, 2022
Managing the Effort:
Insider Threat Program Manager

• Over 23 years working with the US Army as an active duty and civilian counterintelligence (CI) special agent and as intelligence professional and manager.

• Experience with countless CI and Insider Threat inquiries and investigations for the DoD in the US, Europe and deployed in multiple combat zones in support of US contingency operations.

• Selected as the Program Manager for the Insider Threat Program due to background, training and experience.
Managing the Cyber Effort: Senior Subject Matter Expert

- Over 25 years of experience assessing and building programs and expert teams (Fortune 10 through 500 and Gov).
- Experience with handling hundreds of insider threat inquiries; intellectual property theft, economic espionage, PII/PHI theft, insider trading.
- Testified before the U.S. House Committee on Oversight and Government Reform on insider threat and intellectual property theft.
- Senior consultant to public and private sectors.
Typical Insider Threat Program

Per Executive Order 13587, October 2011, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information required to:

• Establish an Insider Threat Program and HUB
• Appoint an Insider Threat Senior Official
• Establish an Information Sharing and Safeguarding Program
• Appoint an Information Sharing and Safeguarding Senior Official
• Appoint a Federal Senior Intelligence Coordinator
**Why Should Everyone be included**

The more employees know and understand their organization has a mature insider threat program and their role in the program the more empowered they feel to contribute by:

• Having more awareness of their importance in spite they may perceive it a small piece

• Understanding what/why certain indicators and outliers could be a potential insider

• Knowing that external adversaries will attempt to elicit information from them no matter how seemingly insignificant, and

• Where and when to report suspected activities.
What Does Training Entail?

Although in this training example we chose elicitation as the subject for this exercise, there are certainly more topics that will provide the right message to the working staffs to include but not limited to:

• Where and when to recognize when a fellow employee may be on the wrong track.

• Knowing the signs of employee(s) behavior that may escalate into potential workplace violence.

• Observing potential systems misuse that could be interpreted as destructive or malicious.
Onto the Training!
What is an “Insider Threat”? 

The stakes are simply too high NOT to report incidents of possible insider threat as soon as they occur.

Insider: Any person with authorized access to any government or contract resource to include personnel, facilities, information, equipment, networks, or systems. This can include employees, former employees, consultants, and anyone with access.

The National Insider Threat Task Force (NITTF) defines an “insider threat” as:

The threat that an insider will use his or her authorized access wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of department resources or capabilities.
NITTF Categories of Insider Threat

LEAKS
SPILLS
ESPIONAGE
SABOTAGE
TARGETED VIOLENCE
Possible Indicators of Insider Threat

Vulnerabilities

Examples of vulnerabilities include:

- Financial stress
- Exploitable promiscuity
- Addictive behaviors
  (e.g., drug/alcohol abuse, gambling, pornography)
- Loneliness
- Disgruntlement
Elicitation Methods – as an example

Why Elicitation Works
A trained elicitor understands certain human or cultural predispositions and uses techniques to exploit them. Natural tendencies an elicitor may try to exploit include:

- A desire to be polite and helpful, even to strangers
- A desire to appear well-informed
- A desire to feel appreciated and believe we are contributing something important
- A tendency to expand on a topic when given praise or encouragement; to show off
- A tendency to gossip
- A tendency to correct others
- A tendency to underestimate the value of the information being sought or given, especially if we are unfamiliar with how else that information could be used
- A tendency to believe others are honest; a disinclination to be suspicious of others
- A tendency to answer truthfully when asked an "honest" question
- A desire to convert someone to our opinion
Elicitation Methods

Do These Techniques Work?

Since the end of the Cold War (1991):

- 67% of spies have been civilians
- 37% had no security clearance
- 84% of spies were successful
- 40% were caught immediately or in less than one year
- 19% were active for five or more years
- 67% volunteered to commit espionage
- 81% received no money for their services
- 94% went to prison

Source: Raytheon’s pamphlet “What Employees Should Know About Elicitation and Foreign Intelligence Approaches”

$300,000,000,000 worth of American intellectual property and business intelligence are annually stolen by China, Russia, Iran, and others.
Catch Me if You Can!

• Nefarious activity associated with transnational criminal groups, nation-state, and fraudster types has surged over the last 5 years.

• With the advent of social media and the like it’s become very easy to connect with people of similar interests. The groups listed above are taking advantage of social media and the cooperative nature of today’s connected society.

• Many recent examples are readily available on the Internet of individuals who have been caught posing as someone else in order to gain something illegally.
Seems Legit!

Claire Divas · 2nd
Professional Freelancer at Xilinx
Srinagar, Jammu & Kashmir, India · 425 connections · Contact info

Highlights
4 Mutual Connections
You and Claire both know Muhamad Elhabbal, Deborah Tang, and 2 others
LONDON (AP) — Katie Jones sure seemed plugged into Washington’s political scene. The 30-something redhead boasted a job at a top think tank and a who’s-who network of pundits and experts, from the centrist Brookings Institution to the right-wing Heritage Foundation. She was connected to a deputy assistant secretary of state, a senior aide to a senator and the economist Paul Winfree, who is being considered for a seat on the Federal Reserve.

But Katie Jones doesn’t exist, The Associated Press has determined. Instead, the persona was part of a vast army of phantom profiles lurking on the professional networking site LinkedIn. And several experts contacted by the AP said Jones’ profile picture appeared to have been created by a computer program.

“I’m convinced that it’s a fake face,” said Mario Klingemann, a German artist who has been experimenting for years with artificially generated portraits and says he has reviewed tens of thousands of such images. “It has all the hallmarks.”
POSSIBLE INSIDER THREAT DETECTED: REPORTED TO ITP

FURTHER INFORMATION REQUIRED

INFORMATION PROVIDED UTILIZED IN ITP INQUIRY

HUB PROCESS

Counterintelligence

Security

Information Assurance/Cyber

Law Enforcement

Office of the Chief Information Officer

Human Resources

Office of the Inspector General

Office of Professional Responsibility

ISSO RECOMMENDS HUB CONVENE

ITP EVALUATES AND REPORTS RECOMMENDATIONS TO ISSO

ACTION TAKEN

ADMINISTRATIVE REFERRAL

LAW ENFORCEMENT REFERRAL (INTERNAL)

SECTION 811 REFERRAL (FBI)

NO ACTION TAKEN

ITP INQUIRY DETERMINATION
Insider Threat – Mature Program

What to watch for:
Categories of activity linked to insider threats

- Network Activity
  - Excessively large downloads
  - Access request denials

- Compliance Cases
  - Noncompliance with training requirements
  - Policy violations

- Data Exfiltration
  - Spikes in outbound email traffic volume
  - Attachments sent to suspicious recipients
  - Removable media alerts

- Time & Expense
  - Expense violations
  - Time entry violations

- Access Attributes & Behaviors
  - Access levels
  - Security clearances
  - Privileged user rights

- Personnel Management
  - Declining performance reviews
  - Notice of resignation or termination
  - Disciplinary action

- Physical Security
  - Physical access request denials
  - Physical access anomalies

- External Data
  - Social media posts
  - Financial duress
  - Criminal/civil history
  - Foreign contacts/travel

= Cyber Area of Responsibility

Typical Cyber Intelligence

• Created processes to better identify and respond to risks and threats.

• Comprised of:
  • Open source (OSINT)
  • Dark web
  • Cyber
  • Insider threat
  • Supply chain risk

• Activities:
  • Cultivate threat intelligence sources
  • Identify & recommend threat intelligence distribution channels and processes
  • Analyze enterprise for newly identified indicators of compromise
The National Threat Task Force (NITTF) released the Insider Threat Program Maturity Framework on November 1, 2018. The Framework is an aid for advancing federal agencies’ programs beyond the Minimum Standards, and builds upon best practices found in the 2017 NITTF Insider Threat Guide. The goal is to help programs become more proactive, comprehensive, and better postured to deter, detect, and mitigate insider threat risk.

NITTF has developed technical bulletins to provide additional information to the insider threat community on technical topics existing within the Insider Threat community. Please review the NITTF Technical Page to view these bulletins.

NITTF has added additional resources to the NITTF Resource Library in the Additional Insider Threat Resources section (formerly known as Briefings to the Insider Threat Community section). Please take some time to review these resources provided by members of the Insider Threat Community.
Resources: Center for the Development of Security Excellence

1. National Insider Threat Awareness Month (NITAM) 2021
2. 2021 Insider Threat Virtual Conference
3. Insider Threat Awareness INT101.16
4. Establishing an Insider Threat Program INT122.16
5. Insider Threat Toolkit
Closing Remarks from FISSEA Chair

Susan Hansche
FISSEA Chair
Cybersecurity & Infrastructure Security Agency
Department of Homeland Security
Complete Survey After Event

https://www.surveymonkey.com/r/FISSEAWinterForum2022
Get Involved

Subscribe to the FISSEA Mailing List
FISSEAUpdates@list.nist.gov

Volunteer for the Planning Committee

Serve on the Contest or Award Committees for 2022
Email fissea@nist.gov
FISSEA Call for Proposals

OPEN year-round

March 18, 2022 – deadline for FISSEA Spring Forum priority consideration

Submit proposals at:
https://www.surveymonkey.com/r/fisseacallforpresentations
REGISTER TODAY

STRONGER TOGETHER

Federal Information Security Educators (FISSEA) Spring Forum

May 17, 2022
1:00pm – 4:00pm ET

#FISSEA2022 | nist.gov/fissea