



# Defense Community Roadmap to Leverage Grants for Enhanced Infrastructure Cybersecurity

---

**7 Nov 2023**

# Panel Members

## Moderator:

**Stacey Shepard - President, Shepard Global Strategies, LLC**

## Speakers:

- **Hon. Lucian Niemeyer - CEO, Building Cyber Security**
- **Daryl Haegley - DAF Technical Director, Controls Systems Cyber Resiliency**
- **Alex Brickner - Dir. SBIR Programs, UMass Lowell Research Institute**
- **Mike Killian – Dir. Strategic Alliances, Cloud Range Cyber**



# *A Defense Community Call to Action...*





**New York Times - May 2023** – “The Biden administration is hunting for malicious Chinese computer code hidden deep inside the networks controlling power grids, communications systems and water supplies **that feed military bases.**”



**“Volt Typhoon”** first detected in telecommunications systems in Guam, is **“a ticking time bomb”** to interrupt or slow American military deployments...But its **impact could be far broader**, because that same infrastructure often supplies the houses and businesses of ordinary Americans.”

# Director of National Intelligence Annual Threat Assessment – 2023

Control systems/critical infrastructure are top “cyber” threats

-  Russia continues to target **critical infrastructure**, including underwater cables & industrial control systems, in US /allied / partner countries, as compromising such infrastructure improves -and sometimes demonstrate -its ability to damage infrastructure during a crisis
-  China can launch cyber attacks that, at a minimum, can cause localized, temporary disruptions to **critical infrastructure** within US
-  Iran has ability to conduct attacks on **critical infrastructure**, as well as to conduct influence and espionage activities. Iran was responsible for multiple cyber attacks between Apr-Jul'20 against Israeli water facilities that caused unspecified short-term effects (*press reporting*)
-  North Korea probably possesses expertise to cause temporary, limited disruptions of some **critical infrastructure** networks and disrupt business networks in US, judging from its operations during the past decade, and it may be able to conduct operations that compromise software supply chains

Adversaries persistently look for any weak link...Which is ours?



# Chinese Targeting U.S. Critical Infrastructure

- DoD's 2023 Cyber Strategy flagged an **uptick in state-sponsored cyber crime** from People's Republic of China (PRC)
- "PRC pose a broad and pervasive **cyberespionage threat**"
- Chinese govt positioning to conduct **disruptive attacks** on American pipelines, railroads, and other critical infrastructure if U.S. gets involved during a potential invasion of Taiwan - *CISA Director Jen Easterly*
- DoD "will leverage all legally available contractual mechanisms, resources, and operational arrangements to improve cybersecurity and expand public-private partnerships."



Released 12 Sept '23

PRC likely intends to launch a destructive cyber attack against U.S. Homeland to hinder military mobilization, sow chaos, and divert attention & resources

# Growing Dark Web Market for OT or 'SCADA Access-As-A-Service' and Access to Critical Infrastructure Orgs

**Продам доступ Водный Округ (Water District) USA**  
Selling Access to US Water District  
Have over 20k clients in two cities  
Posted 8 hours ago  
18 hours ago, vasyldn said:  
Florida, USA Gov network - domain admin - 6000\$  
SOLD

**Florida, USA Gov network - domain admin - 6000\$**  
SOLD

**電力系統**  
I have access to SCADA servers. Who can tell how and for what you can use this for? The country is China.

**stallman**  
I always buy accesses to American hospitals, and other US medical infrastructure, these are the most priority goals for me at the moment for the purchase. In addition, access to any US government infrastructure is interesting, the larger the better, but schools, fire stations, police stations and other small stuff is also acceptable  
In addition, at the moment, I am interested in accesses to hospitals, manufacturers of medical equipment and to anything somehow related to medicine from AU, CA, UK, EU. If you have something medical from other countries - let me know, maybe I'll buy it too.

**[Up to 500k\$]Куплю PoC удалённого запуска кода на IOT.**  
[Up to \$500k] I will buy PoC of remote code execution on IOT  
We pay quickly and a lot  
Each offer is evaluated individually, depending on the complexity of implementation, the number of devices on Shodan, and GEO (USA/UK/DE/CA/FR/AU/IT)  
Write immediately on the case – offer and price, be prepared for a demonstration

2024

# *Report on Critical Infrastructure Supporting National Security and Force Projection Activities*

- Committee commends DOD on efforts to address cyber vulnerabilities of servicemembers, military installations, the defense industrial base, and other key components of the national security enterprise. The committee remains concerned, however, about the potential for cyberattacks against the homeland to impede ability of DOD to conduct operations and functions. **DOD must do more to address domain awareness gaps to ensure that vulnerabilities to military installations, which stem from dependence on critical infrastructure located in surrounding communities, do not present an attack vector which adversaries can exploit.** Therefore, SECDEF, in coordination with MILDEPS, NGB & DHS, a report to SASC & HASC NLT **01 Feb 24**, on **vulnerabilities of military installations related to critical infrastructure supporting national security and force projection activities.**
- Report shall include:
  - (1) **Development of potential models** for establishing processes, relationships, and command structures for proactively identifying vulnerabilities, responding to cyber incidents involving DOD installations, and providing synchronized reporting to higher authorities;
  - (2) **An assessment of the feasibility of designing and establishing a data repository** within the DOD for resources and data related to potential cyber incidents involving DOD installations; tailored responses; impacts; and exercises to facilitate the sharing of policies, procedures, best practices, data, and emerging issues; and
  - (3) **An assessment of the need for utilizing the planning and execution of integrated campaigning** (as defined in the Joint Chiefs of Staff Joint Concept for Integrated Campaigning) at multiple echelons to understand potential adversary actions against U.S. Government and non-government partners and to better inform campaign plan assumptions.

# Response - ADC OT Cyber Working Group

- **Raise awareness with respect to cyber security risks to critical infrastructure**
- **Garner best practices from those communities actively engaged with their installations**
- **Share success stories with those looking to improve their cyber safety**
- **Identify funding resources to enable initiatives**
- **Promote training and educations for workforce development**





# Case Study: UMLARC Cyber Fusion Center



Map what is there  
**Critical  
Infrastructure  
Information System**  
(CIIS)



Train more people to map  
**Community Cyber  
Force**  
(CCF)



Put the maps to use  
**Defense Community  
Research Network**  
(DCRN)

**Secure Location  
Community Cyber Support Facility (CCSF)**

# Expanding Partnerships at Hanscom AFB



## Secure Location Community Cyber Support Facility (CCSF)

- **Funded by the Defense Community Infrastructure Pilot Program (DCIP)**
- Providing visibility into infrastructure risks that could impact installation mission assurance
- Facilitating cyber mutual aid through a cyber workforce in secure facilities
- Providing secure facilities for collaboration with local defense and small business community

**Coming Winter 2023**

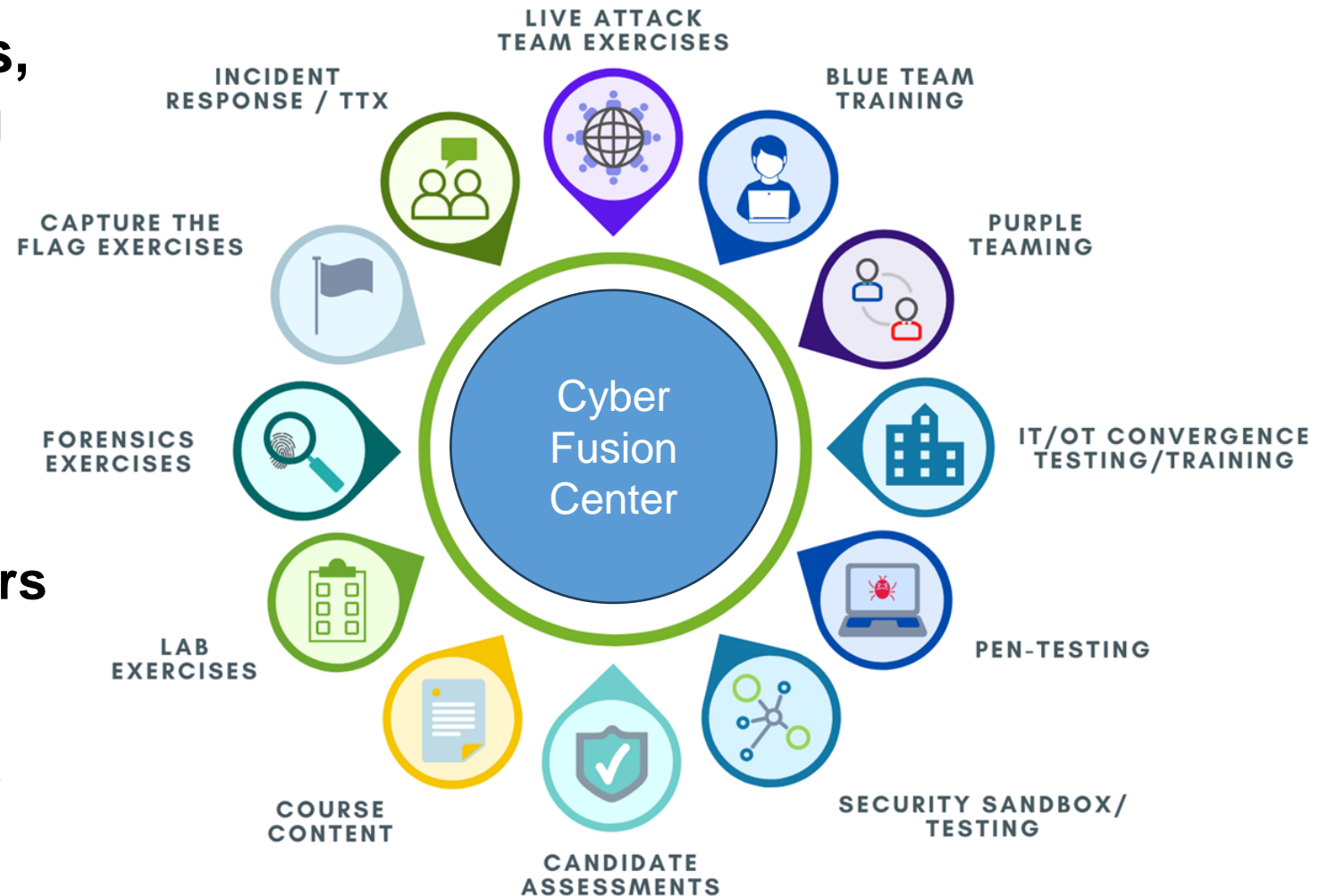
"Cybersecurity is critically important for Hanscom now, and it will continue to be so in the future. Increasing threats to our nation from criminal and nation-state actors reinforce the growing need for collaboration, communication, and a whole-of-community approach to defending and responding to cyber incidents."

Taona A. Enriquez, Colonel, USAF Commander 66<sup>th</sup> ABG

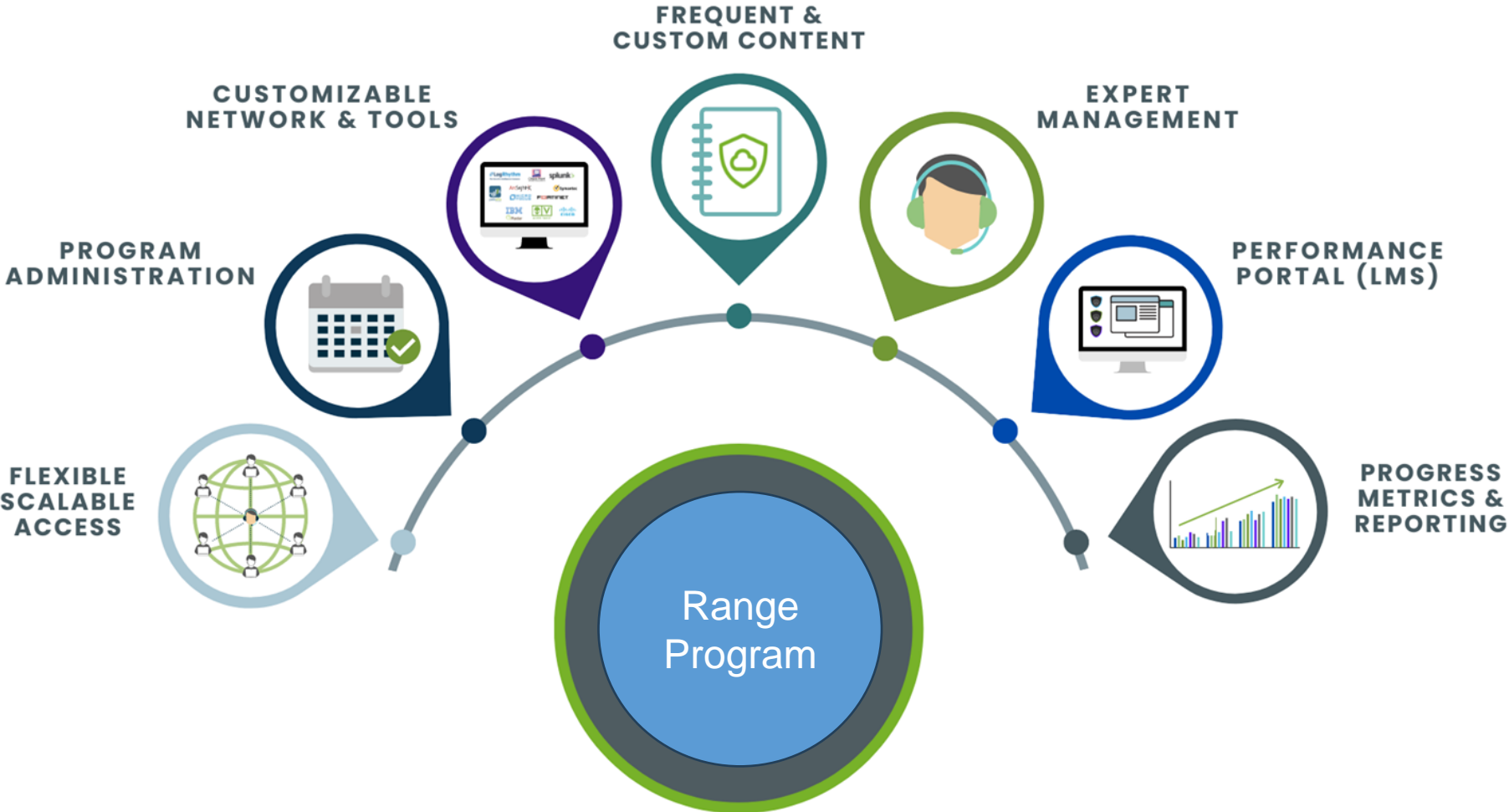
# The CCSF - A “Cyber Fusion Center”

**Bringing Cyber Capabilities, Collaboration, and Training together...for all Defense community stakeholders**

- **Military Installations**
- **Utilities (power, water, comm)**
- **Emergency First Responders**
- **Disaster Recovery Teams**
- **Local Governments**
- **State and Federal Agencies**



# PERSISTENT CYBER TRAINING ENVIRONMENT (PCTE)



# Case Study: State of Florida

---

## Problem Domain:

Statewide need to improve cyber readiness for State Employees to recognize and defend against increasingly more sophisticated cyber attacks

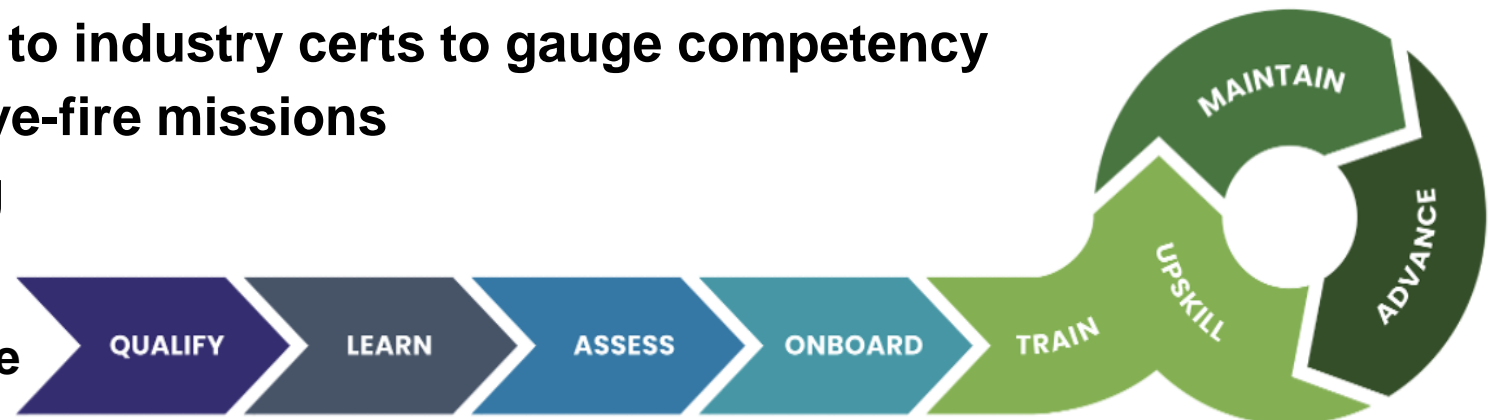
## Solution:

- Provide live and skills gap training to improve Cyber Readiness utilizing current threats

## Execution:

- Prescribed Learning paths mapped to skill gaps
- 1500+ self-service Labs mapped to industry certs to gauge competency
- Instructor-facilitated missions live-fire missions
- Performance Portal for reporting

The Cyber Learner Lifecycle



# Bottom Line

**Defense communities must become more active in the coordinated protection of critical infrastructure providing essential services for national security and life supporting functions**

**Cyber Resilience is a critical factor for Military Value**

**Looking for more information on the grants used for the CCSF?**



# *Case Study Points of Contact*

- **Grant for Community Cyber Support Facility (CCSF)**

**Alex Brickner**

Email: [alex\\_brickner@uml.edu](mailto:alex_brickner@uml.edu)

Phone: 847-275-5327

- **State of Florida Cyber Readiness Training**

**Mike Killian**

Email: [mkillian@cloudrange cyber.com](mailto:mkillian@cloudrange cyber.com) Phone: 770-843-3673