REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
12-06-2019	Technical Report	

4. TITLE AND SUBTITLE

AF CyberWorx Event:
Smoke VPN

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

AF CyberWorx
2354 Fairchild Dr, Ste 4A41
USAF Academy, CO 80840

8. PERFORMING ORGANIZATION REPORT NUMBER

19-002

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AF CyberWorx
2354 Fairchild Dr, Ste 4A41
USAF Academy, CO 80840

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

24th Air Force asked AF CyberWorx to facilitate and host a CyberNext technology discovery and networking event 5 February 2019. Government and industry participants explored the technologies and operational use cases of the SmokeVPN system that use a streaming one-time key protocol and implements port/route hopping. The group explored three specific use cases to serve as a foundation for further operational testing of the system.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Michael V. Chiaramonte, Lt Col, Director
UU	UU	UU	UU	12	19b. TELEPHONE NUMBER *(Include area code)* (719) 333-3399

AIR FORCE
CYBERWORX™

AIR FORCE CYBERWORX REPORT 2019-02

Smoke VPN

MS. VELVADA PRESTON
Senior Designer & Facilitator

MICHAEL M. HELGESON Lt Col, USAF
Project Lead

MICHAEL V. CHIARAMONTE, Lt Col, USAF
Director, AF CyberWorx

DESIGN PROJECT CONDUCTED
5 February 2019 (CyberNext)

Produced with input from numerous units including 24AF/TO, 688 CW/TA, 561 NOS, and our valuable partners in industry.

Air Force CyberWorx™
2360 Vandenberg Dr, Ste 4A41
USAF Academy, CO 80840
AFCyberWorx@usafa.edu - @AFCyberWorx - (719) 333–3399

Introduction to AF CyberWorx

Air Force CyberWorx is a dynamic organization partnering Airmen, industry, and academia to reimagine how technology might enrich and protect our nation, businesses, and lives. As a human-centric design center, we seek out unique ways to connect Air Force warfighters with current and future technology in meaningful ways. We look to transfer, license, and share promising prototypes, solutions, and knowledge with our partners to create value for both the warfighter and the economy as this is the best way toward operational advantage.

Design Thinking at AF CyberWorx

Design thinking is a common sense, human-centered, problem-solving method embraced by industry leaders such as Apple and Google but it's often overlooked in the government sector. The AF CyberWorx design thinking process is a multidisciplinary method that breaks down silos of standard organizational structures. Organizations naturally form structures based on specializations to facilitate deep expertise, but these structures often impede the creativity, collaboration, and knowledge sharing that is vital to innovation. AF CyberWorx deliberately reaches across specialties to bring diverse perspectives to a problem in a non-threatening environment. This evokes ideas that would otherwise be missed or stifled. The multidisciplinary design approach teases out meaningful solutions that are intuitive and desirable to Airmen.

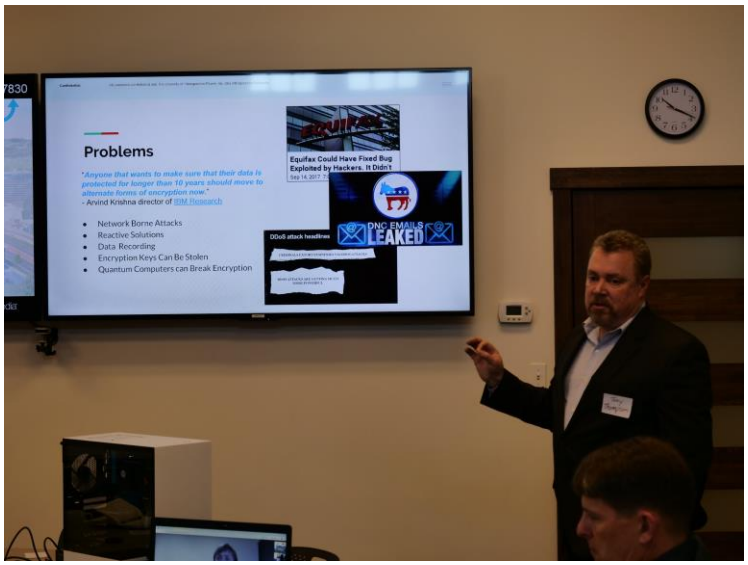
Air Force CyberWorx offers facilitated design thinking sessions that bring industry and academic experts together with stakeholders to develop solutions to hard problems. These sessions are tailored to best meet Air Force needs with differing lengths based on time sensitivity and Air Force CyberWorx capacity.

Air Force CyberWorx was asked by 24th Air Force to facilitate and host a session focused on exploring the technologies and operational use cases of SmokeVPN which is under development by Introspective Networks. Toward that end, AF CyberWorx staff, while working together with the Center for Technology, Research, and Commercialization (C-TRAC) brought together a diverse group of Air Force professionals to examine the technology during a CyberNext™ event.

Design Problem

The design question for the CyberNext event was straightforward: How might we best operationally leverage a VPN system that uses a streaming one-time key protocol and implements port/route hopping.

The group met on 5 February at Catalyst Campus, where key leadership from Introspective Networks provided an overview and answered questions regarding SmokeVPN's technologies and capabilities. Ultimately, the group determined the value proposition in Introspective Network's SmokeVPN lies in its implementation of Streaming Transmission One-time-pad Protocol (STOP) to create a virtually unlimited key size and transfer key data physically and temporally out of synchronization with data streams. This provides protection against not only current cryptanalysis methods but the potential to defend against the future capabilities envisioned by quantum computing. Additionally, SmokeVPN's use of port/route hopping on both key and data streams claim to provide a defense against most traditional network-borne attacks. Introspective Networks closed their presentation with a demonstration of their SmokeVPN in action, a moving target defense, uptime log, and ping latency displayed.



Theme Discovery

With these advantages in mind, the group set off to brainstorm possible operational use cases within the Air Force using some key design-thinking methodologies covering ideation, refinement, and concept evaluation.

The team came up with a large number of possible opportunities for SmokeVPN to enhance secure communications for current and future Air Force missions which fell broadly into three categories:

- Remote Access Services (RAS)
- Point-to-Point Links (P2P)
- Legacy System Security

The group then considered all of the ideated use cases based on which could have the largest mission impact, would be the easiest to field, and piqued the most interest because of personal experience with the problem domain. Using these criteria, they chose three specific use cases to explore in-depth:

- Encrypted data channels used to transfer email (server-to-server & server-to-client)
- Enhance security of critical infrastructure (ICS, SCADA, etc)
- Enhance security of legacy weapon systems

Encrypted data channels to transfer email between servers and from server to clients

The group identified that the Air Force needs a better way to share sensitive information so that PII FOUO information is properly protected. Which benefits the Air Force by ensuring regulatory compliance and liability protection. When left to the user, sensitive information could be missing and sent unprotected. Encrypting all email could solve this problem, but the overhead costs in terms of time, storage, and processing is unacceptable and creates challenges with accessing legacy data encrypted with deprecated or revoked keys. This particular use case and ideation sessions did not fully address email originating outside the Air Force network or being transmitted to outside networks.

Impact	Tech Requirements
• Encrypting everything will remove user decision/error and ensure 100% compliance	• "Handful" of email servers client software.
Gaps	**Action**
• Integration with current system integration with CHES/OWA. Uknown requirement for future AF/DOD cloud infrastructure	• Use technology to encrypt all email using less bandwidth and time.

Enhance Security of critical infrastructure (ICS, SCADA, and other control systems)
The group identified that the Air Force could implement secure, remote, centralized control and monitoring of critical infrastructure across the force. This requires a better way to control and query critical infrastructure systems (not designed or planned to be integrated into the enterprise) while protecting it from adversary effect. This would allow the Air Force to take advantage of disparate, stove-piped data to conduct preventative monitoring and maintenance of critical infrastructure while leveraging automation and facilitating data aggregation/analysis.

Impact	Tech Requirements
• Enables automation and remote operations • Trend analysis and predictive MX	• VPN device at CPE • HW/SW at each node • Specific adapters/interfaces • Authority/Strategy to seal (A4/7) • Business case to support/justify
Gaps	**Action**

• IIP/integration with VPN
• Validate vendor confidence in VPN
  ○ Security and performance buy-in
• Local authority for test
  ○ ID permission-granting authority
	• Identify use case local to 24AF
	• Seek authority/permission to test
	• Build support among A4/A7 communities for test of initial system and automation/data-driven management
	• Execute test and conduct analysis for expanded use

Enhance Security of Legacy Weapon Systems
Many legacy weapon systems were built as their own isolated enclave and do not have the innate security required to allow greater networking and collaboration between echelons and across service components. The Air Force needs a way to secure cyber weapon systems data so that

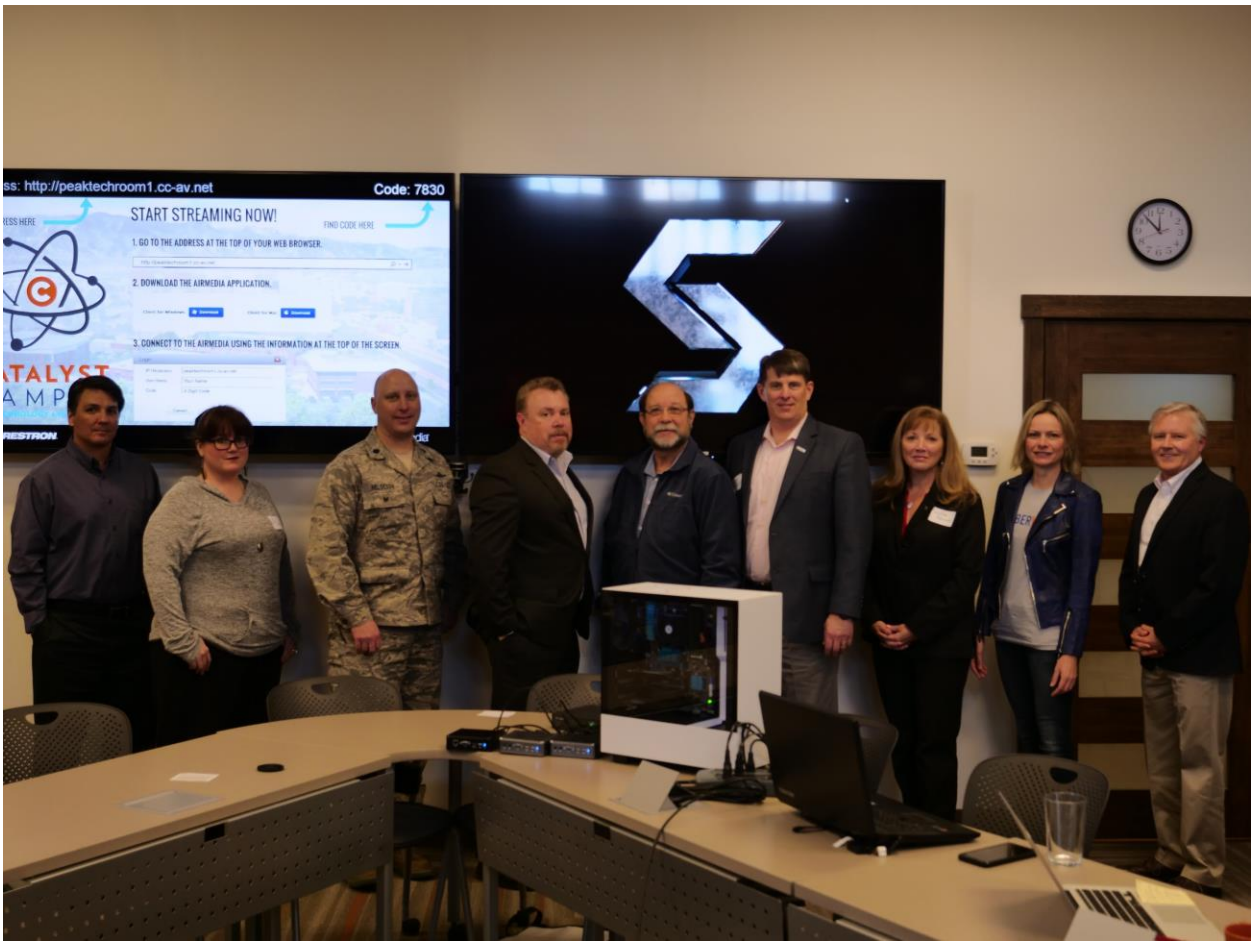
remoted operations data can be securely linked to/from Garrison. This will benefit Air Force Cyber by providing a high speed, secure link between remote and central locations.

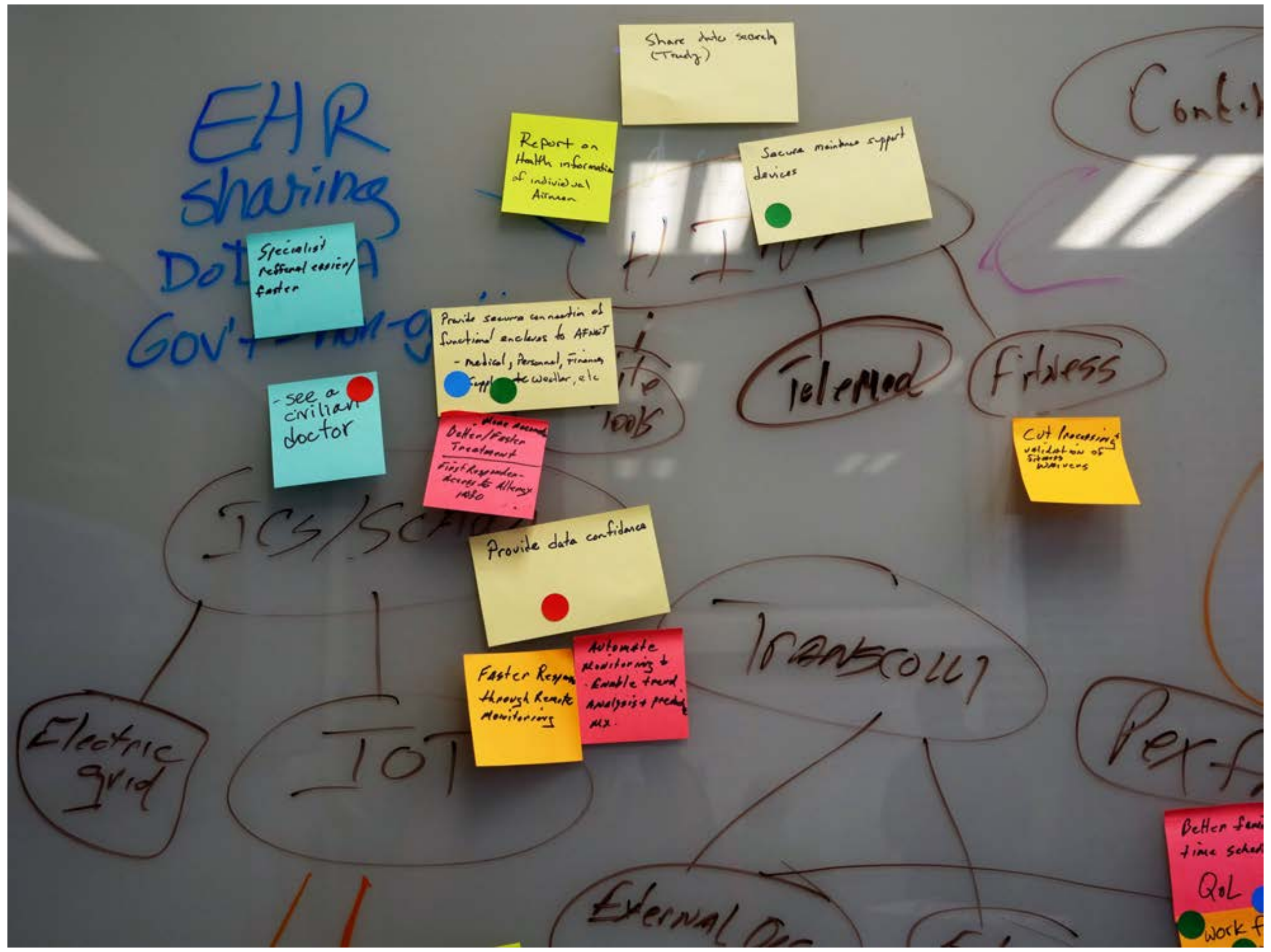
Impact	Tech Requirements
• Greater transfer rate • More reliable/secure	• Limited scope (base to base) • Smoke Wall
Gaps	**Action**
• AFNet policies/capabilities • Interim Authority to Test • CPT or Weapon Systems • Contracting Vehicle	• Work through the gap analysis problems and find ways to address them

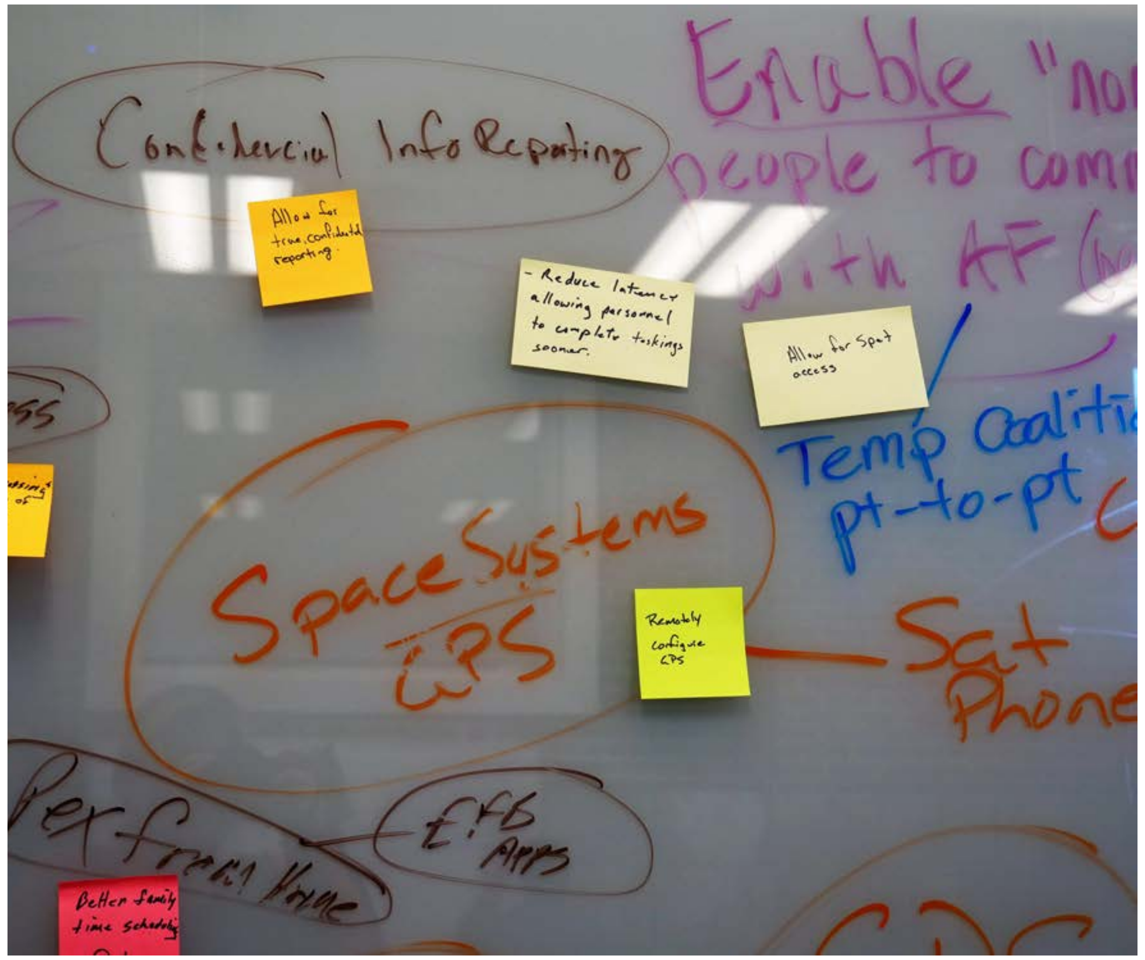
Next Steps

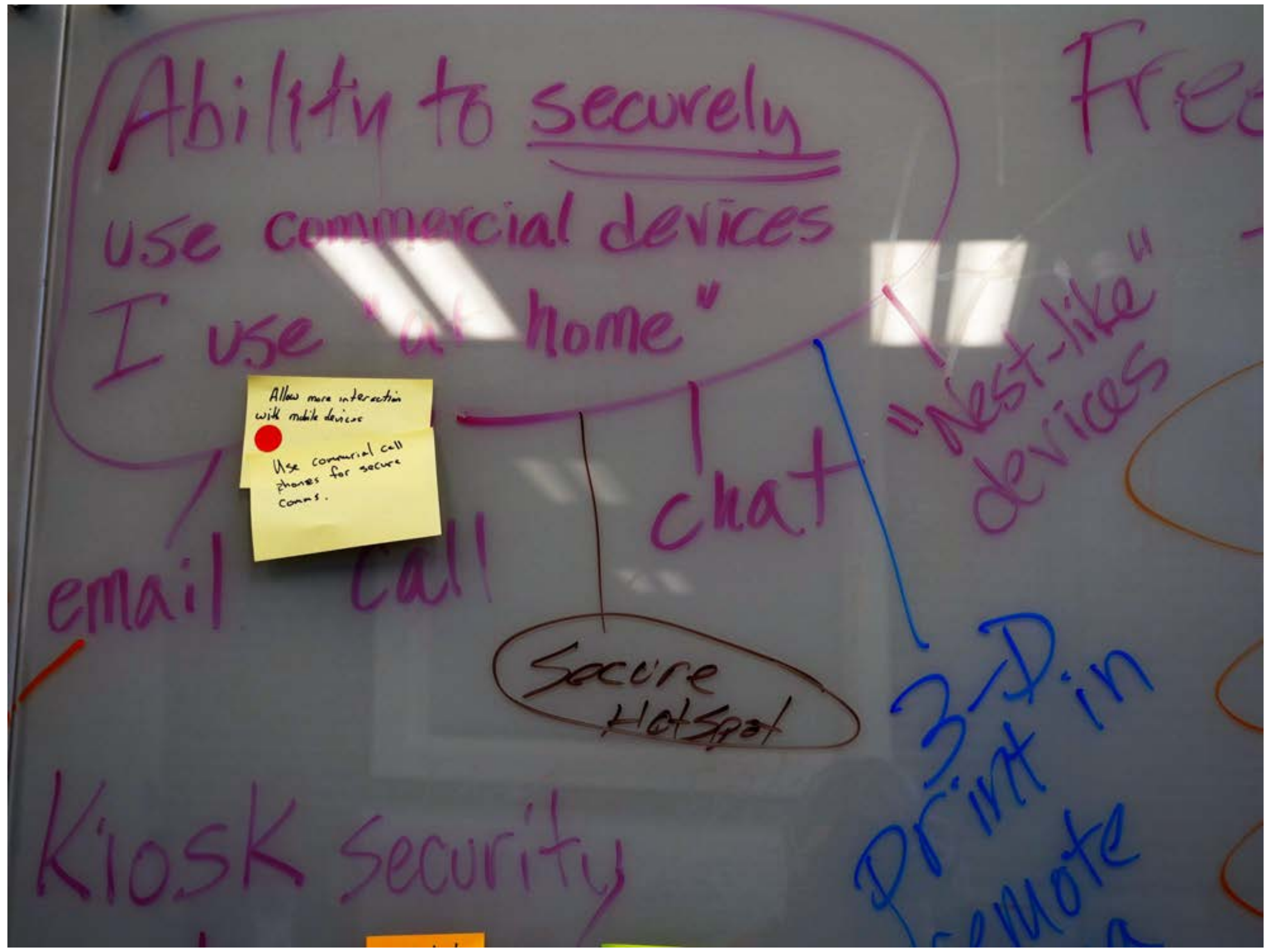
Introspective Network's presentation of SmokeVPN demonstrated its functionality and explained the key attributes of its technology that make it different from other communications security technologies. The group's exploration of these capabilities produced a large number of opportunities to enhance the Air Force mission with significant and enduring impact. The three specifically explored use cases could serve as the foundation for further operational testing of the system. Since this is already a commercially viable solution, Air Force CyberWorx recommends the following:

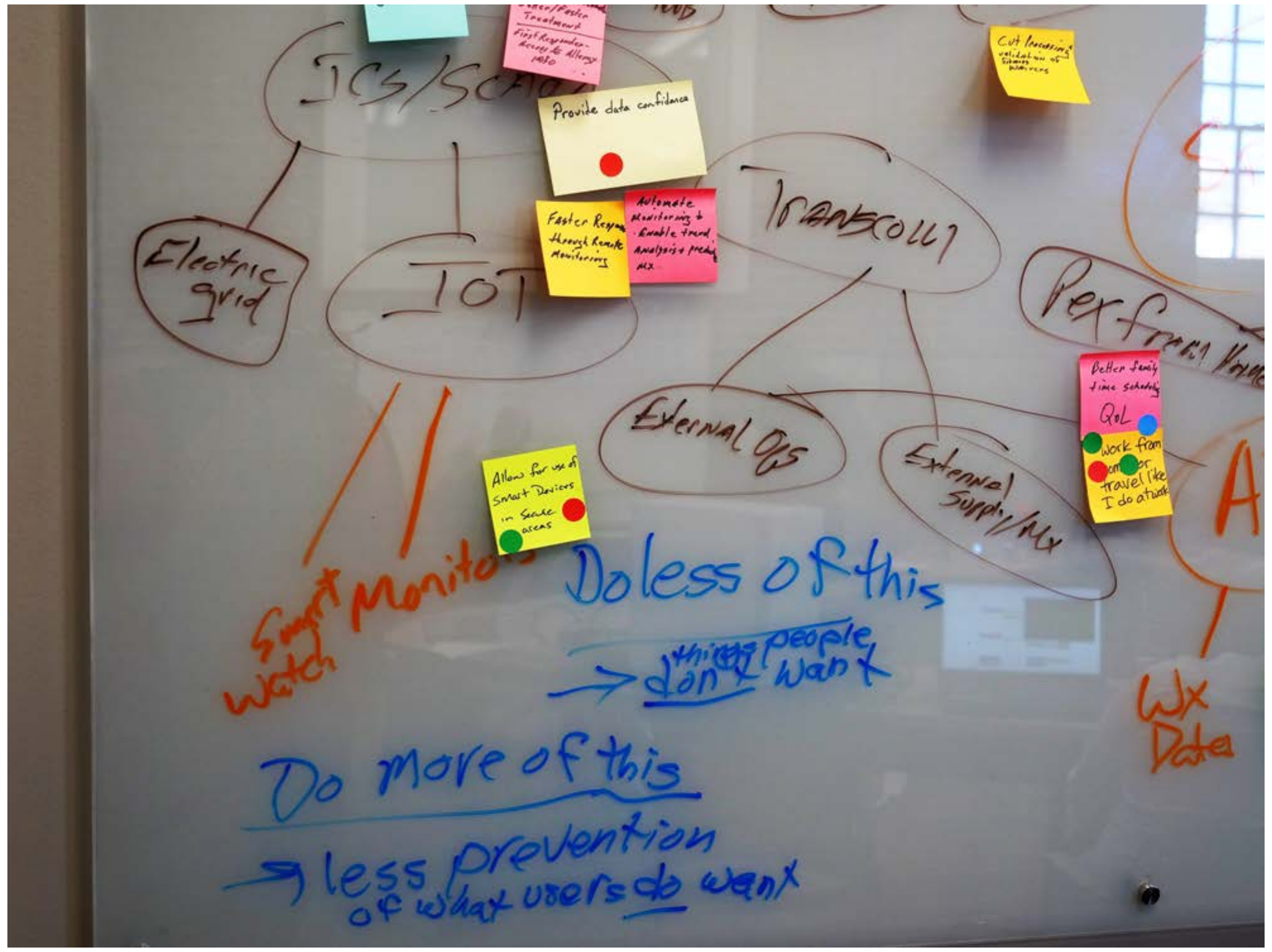
1. The solution be technically evaluated to:
    a. Confirm security viability in an Air Force operating environment.
    b. Confirm the stated benefits of the technology are realized in an operational environment.
2. Determination of ROI based on results of technical tests in #1.
3. Select use case and execute pilot deployment if ROI is positive.

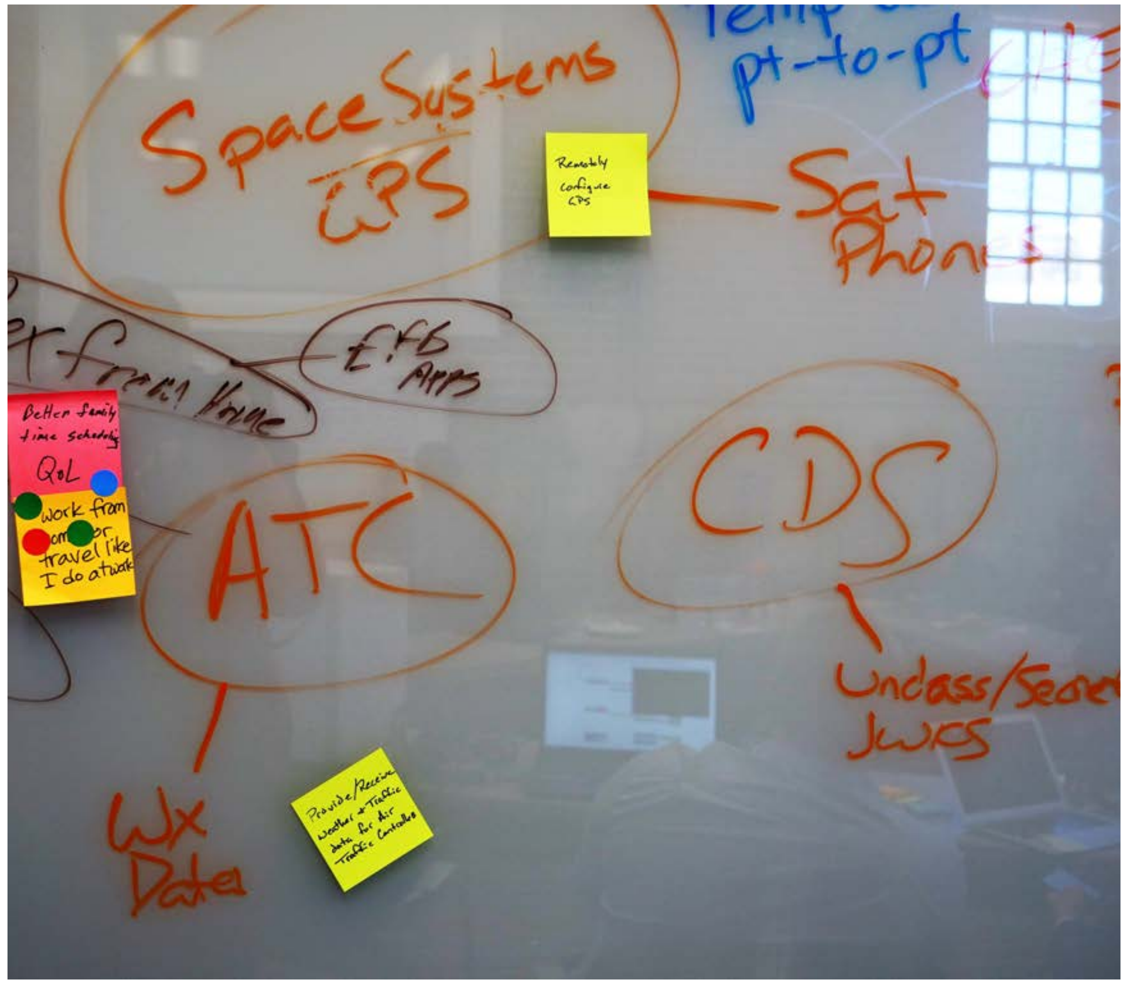

http://peaktechroom1.cc-av.net
Code: 7830
START STREAMING NOW!
1. GO TO THE ADDRESS AT THE TOP OF YOUR WEB BROWSER.
2. DOWNLOAD THE AIRMEDIA APPLICATION.
3. CONNECT TO THE AIRMEDIA USING THE INFORMATION AT THE TOP OF THE SCREEN.


EHR sharing
Report on Health information of individual Airmen
Secure maintain support devices
TeleMed
Fitness
- see a civilian doctor
Provide data confidence
Faster Response through Remote Monitoring
Automate Monitoring & Enable trend Analysis predict MX
Electric grid
IOT
Better family time scheduling
QoL

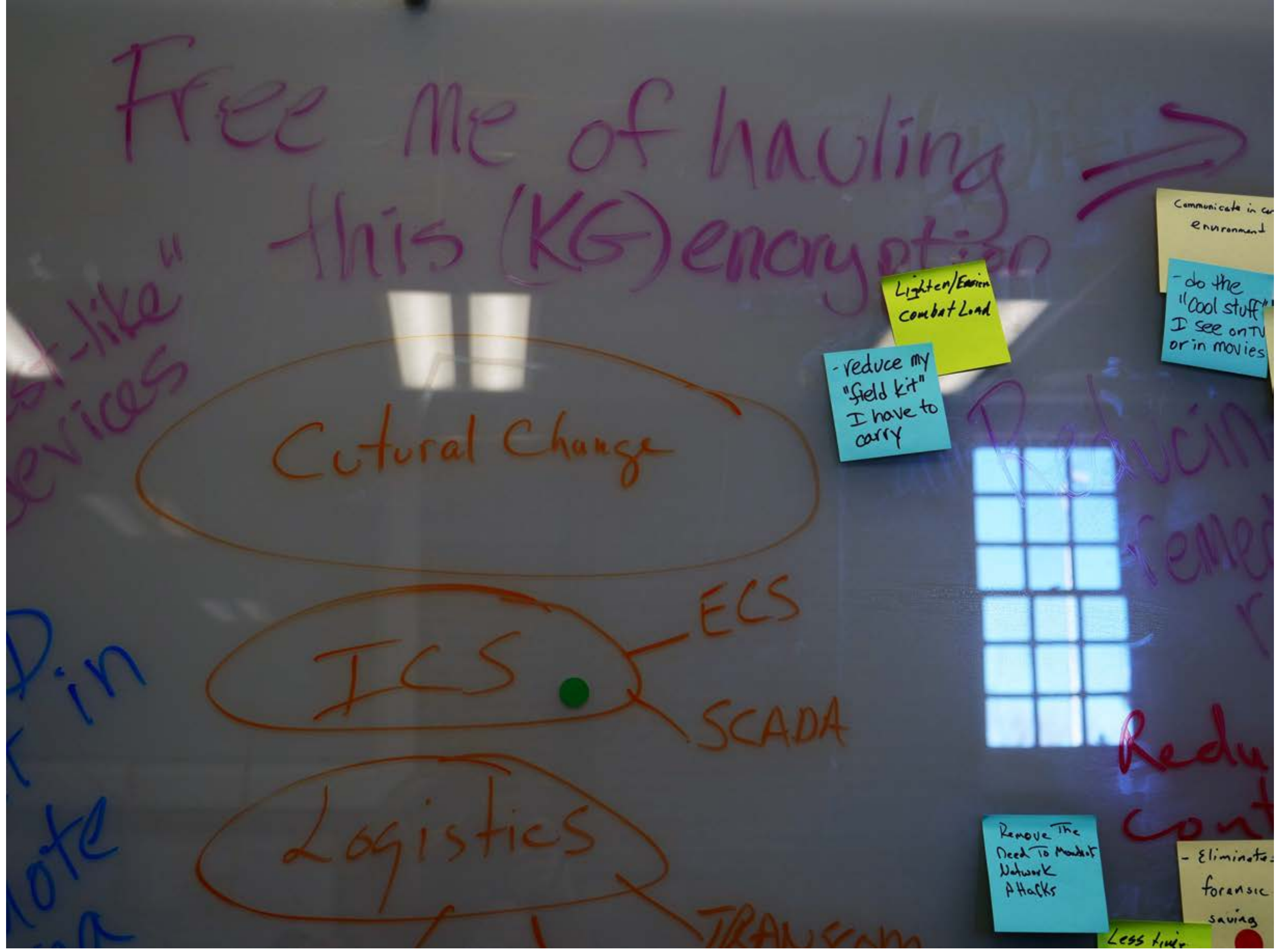
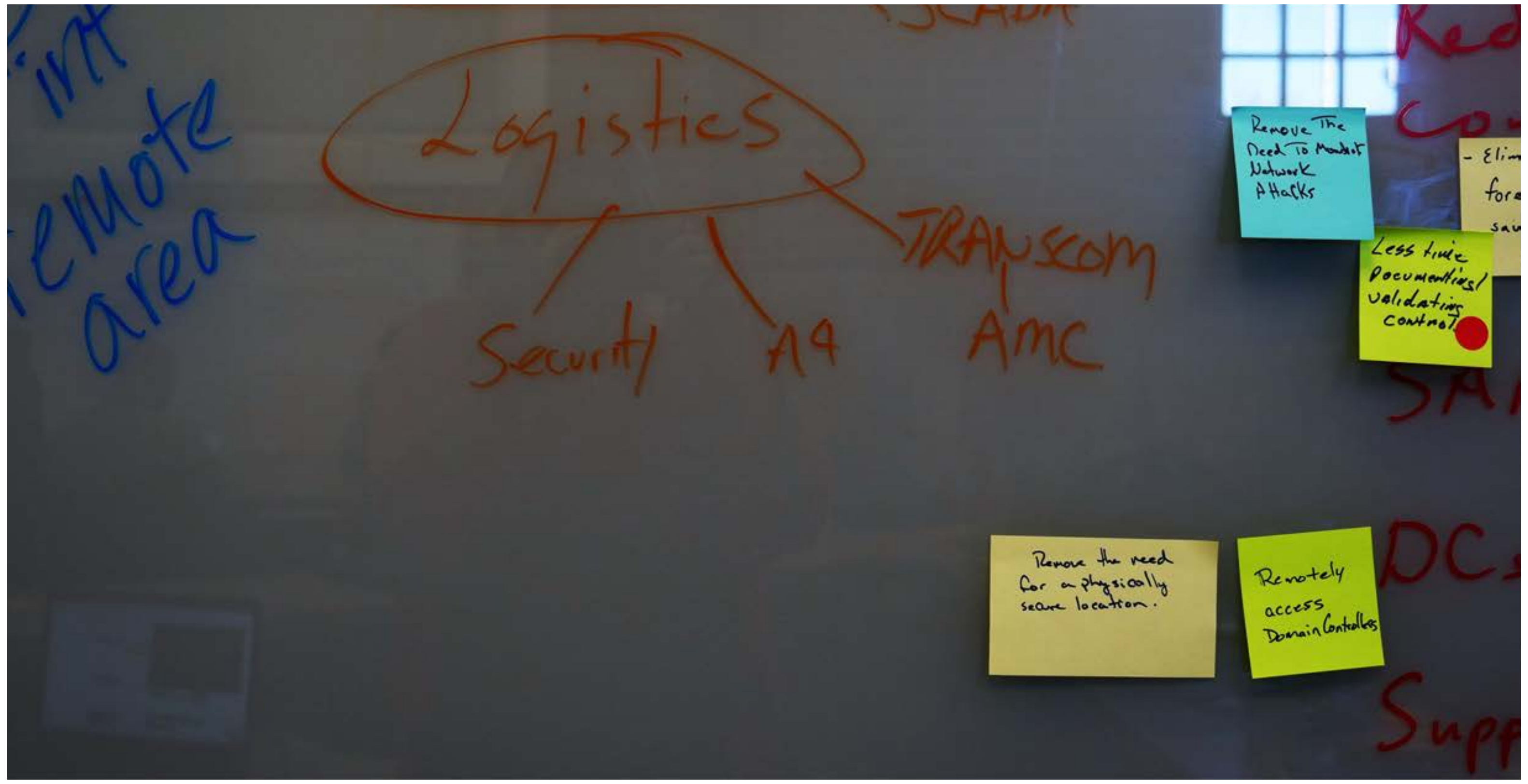
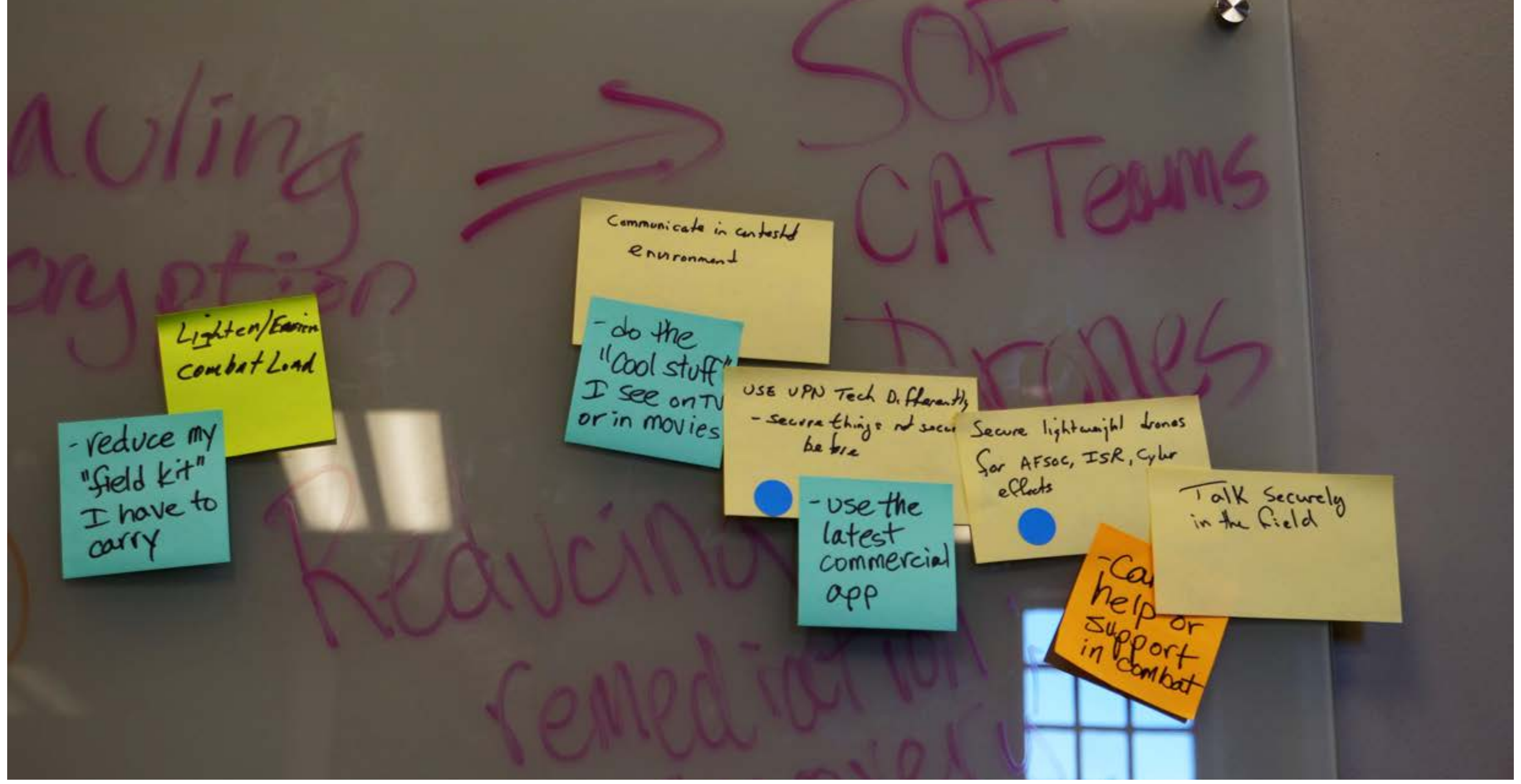
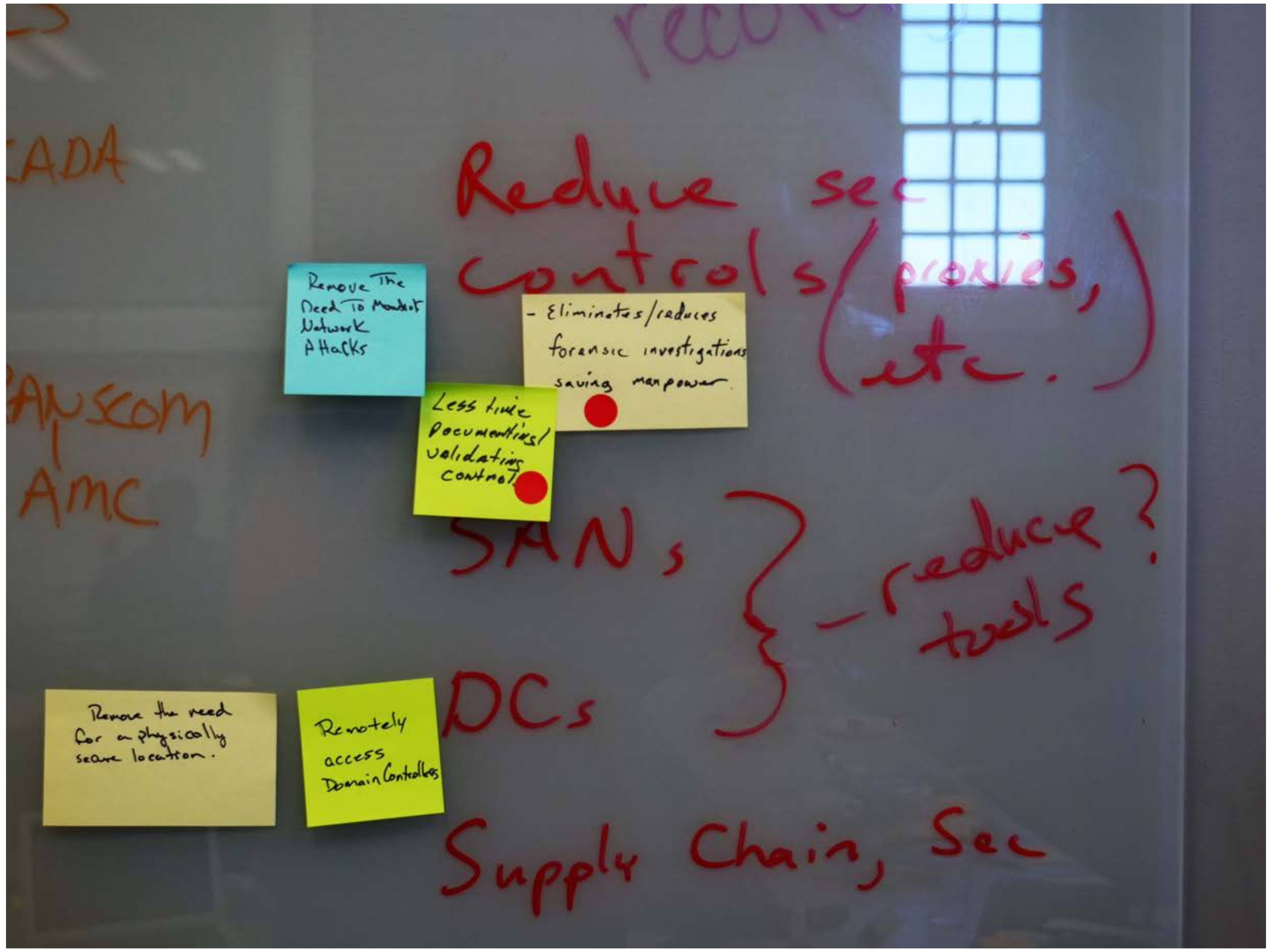

Confidential Info Reporting
Enable
people to
Allow for true, confidential reporting
- Reduce latency allowing personnel to complete taskings sooner.
pt-to-pt
Space Systems
GPS
Remotely configure GPS
Sat Phone
EFB Apps
Better family time scheduling

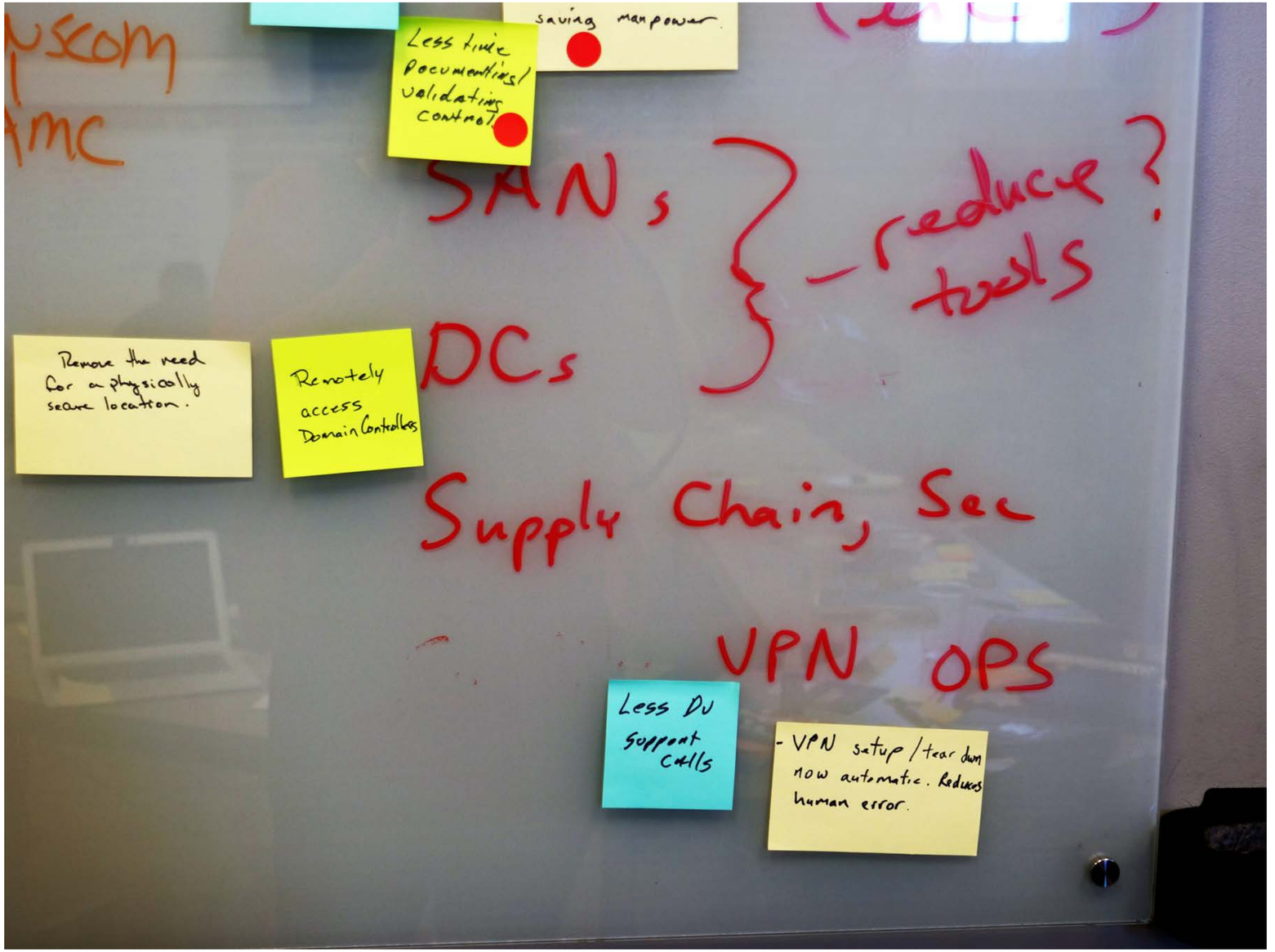

Ability to securely use commercial devices I use "at home"
Allow more interaction with mobile devices
Use commercial cell phones for secure comms.
email
call
chat
"Nest-like" devices
Secure Hotspot
Kiosk security
3-D print in


Provide data confidence
Electric grid
IOT
External Ops
Better family time scheduling
QoL
work from
travel like I do at work
Allow for use of Smart Devices in secure areas
Smart Watch
Monitor
Do less of this
→ things people don't want
Do more of this
→ less prevention of what users do want
Wx Data

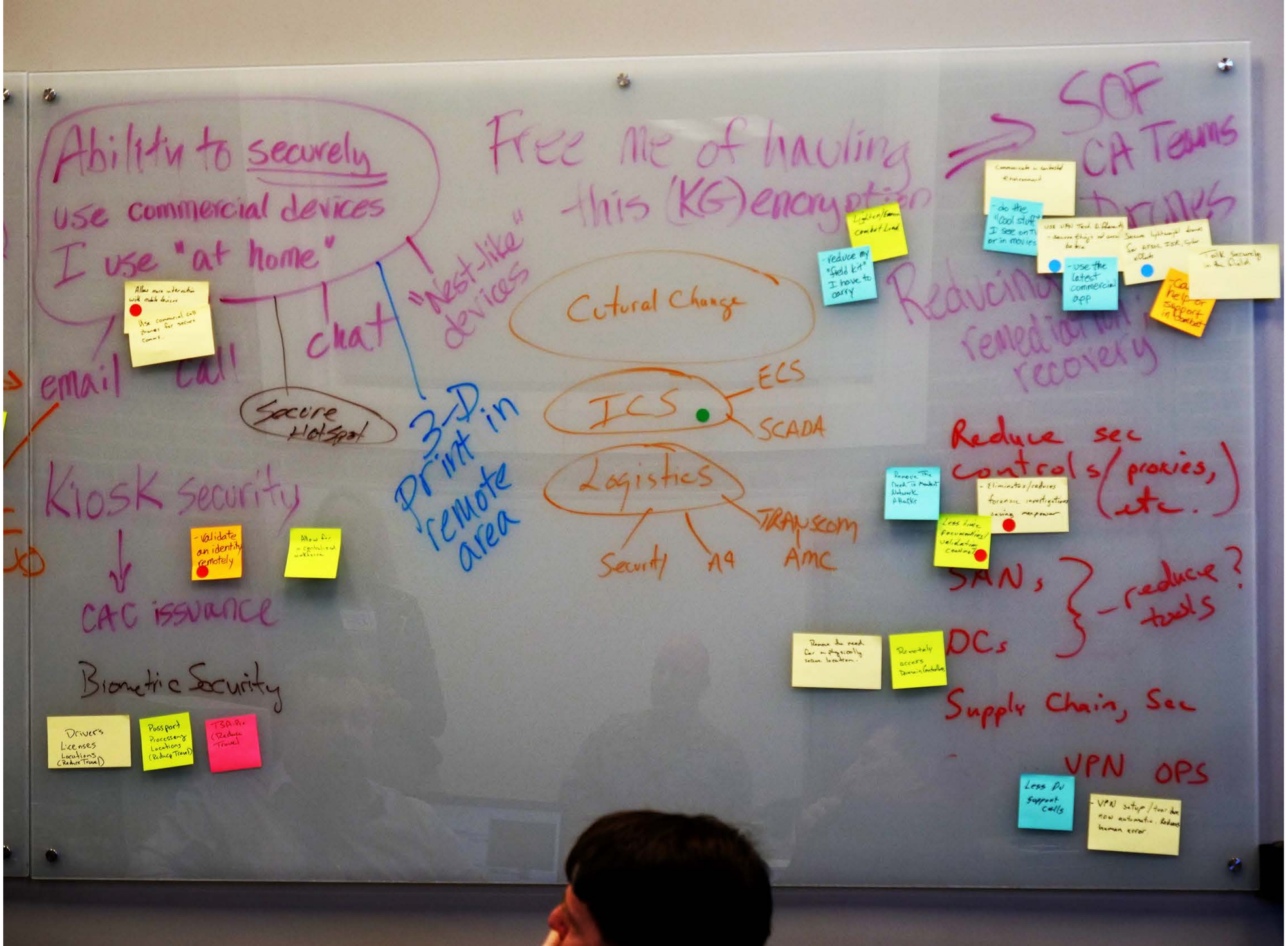

Space Systems
GPS
Remotely configure GPS
pt-to-pt
Sat Phone
EFB Apps
Better family time scheduling
QoL
work from
travel like I do at work
ATC
CDS
Wx Data
Provide/Receive weather & Traffic data for Air Traffic Controllers


email
call
chat
Secure Hotspot
3-D print in remote area
Kiosk security
- Validate an identity remotely
Allow for a centralized workforce
CAC issuance
Biometric Security
Drivers Licenses Locations (Reduce Travel)
Passport Processing Locations (Reduce Travel)
TSA-Pre (Reduce Travel)


Free me of hauling this (KG) encryption
Cutural Change
ICS
ECS
SCADA
Logistics
Lighten/Ease combat Load
- reduce my "field kit" I have to carry
- do the "cool stuff" I see on TV or in movies
Remove The Need To Monitor Network Attacks

Logistics
Security
A4
TRANSCOM
AMC
remote area
Remove The Need To Monitor Network Attacks
Less time Documenting/ validating control
Remove the need for a physically secure location.
Remotely access Domain Controllers

SOF
CA Teams
Drones
Reducing remediation
Communicate in contested environment
Lighten/Ease combat Load
- reduce my "field kit" I have to carry
- do the "cool stuff" I see on TV or in movies
Use VPN Tech Differently
Secure lightweight drones for AFSOC, ISR, Cyber effects
- Use the latest commercial app
Talk Securely in the field
help or support in combat

Reduce sec controls (proxies, etc.)
SAN,
DCs
- reduce tools?
Supply Chain, Sec
Remove The Need To Monitor Network Attacks
- Eliminates/reduces forensic investigations saving manpower
Less time Documenting/ validating control
Remove the need for a physically secure location.
Remotely access Domain Controllers


Less time documenting/ validating control
saving manpower
SANs
DCs
reduce tools?
Remove the need for a physically secure location.
Remotely access Domain Controllers
Supply Chain, Sec
VPN
OPS
Less DU support calls
- VPN setup / tear down now automatic. Reduces human error.


EHR sharing
Confidential Info Reporting
Enable "non-AF" people to communicate with AF (because now securable)
Temp Coalition pt-to-pt
CHES
Telemed
Fitness
Electric grid
External Ops
Space Systems
Sat Phones
ATC
CDS
Unclass/Secret JWICS
Wx Data
Smart Watch Monitors
Do less of this
→ things people don't want
Do more of this
→ less prevention of what users do want
PII FOUO
email
Kiosk
Allow for Spot access
Reduce latency allowing personnel to complete taskings sooner.
see a civilian doctor
Remotely configure GPS
Send email that contains PII or FOUO w/out an added step
share sensitive info (with less risk)
Drivers Licenses Locations (Reduce Travel)
Passport Processing Locations (Reduce Travel)


Ability to securely
use commercial devices
I use "at home"
email
call
chat
Secure Hotspot
"Nest-like" devices
3-D print in remote area
Free me of hauling this (KG) encryption
Cultural Change
ICS
ECS
SCADA
Logistics
Security
A4
TRANSCOM
AMC
Kiosk security
CAC issuance
Biometric Security
Drivers Licenses Locations (Reduce Travel)
Passport Processing Locations (Reduce Travel)
TSA Pre (Reduce Travel)
- validate an identity remotely
- do the "cool stuff" I see on TV or in movies
- use the latest commercial app
- reduce my "field kit" I have to carry
SOF
CA Teams
Drones
Reducing
remediation
recovery
Reduce sec controls (proxies, etc.)
SANs
DCs
reduce tools?
Supply Chain, Sec
VPN OPS
Less PW support calls
- VPN setup/test now automatic. Reduced human error