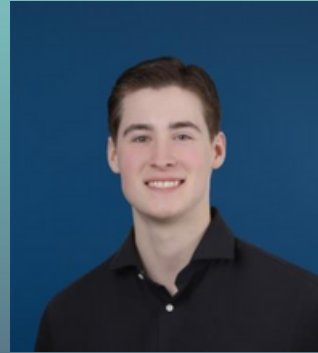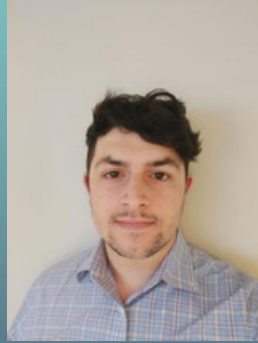# Hacking for Diplomacy
DS 25 -Outsmarting Smart Devices

Meet The Team

Mitch Lamosek, Sierra Kennedy, Arthur Tonoyan, Camden Robertson, Jacob Herman
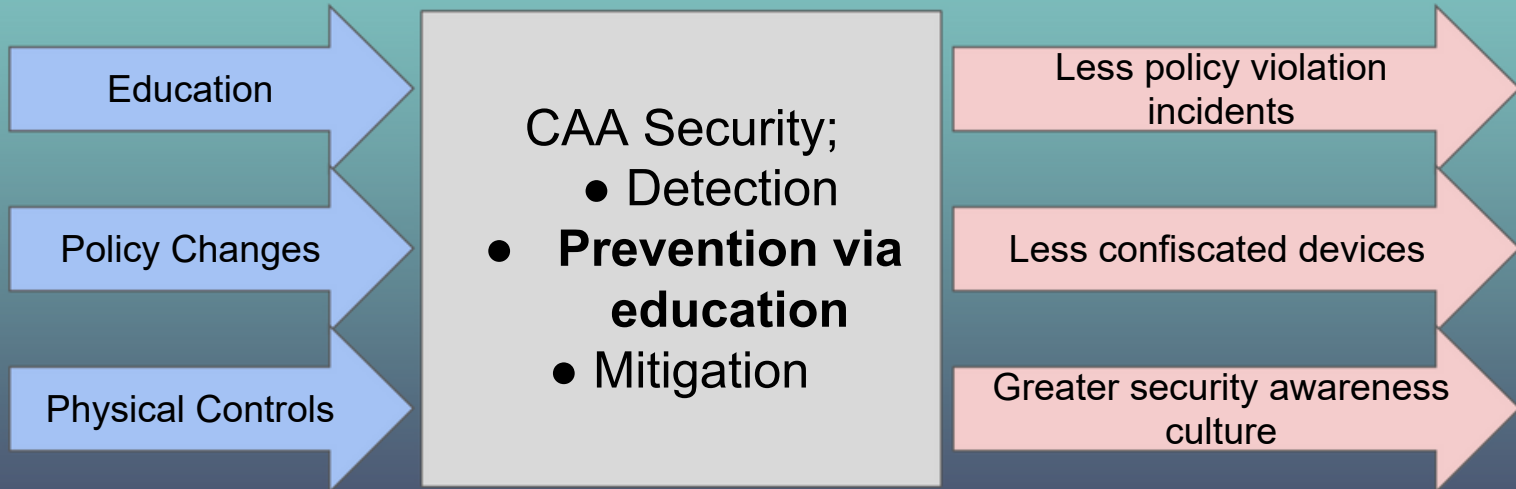
Initial Problem Statement

Foreign Service Officers (FSOs) at the U.S. Tri-Mission Brussels need to be alerted when they inadvertently bring personal devices, which may contain unauthorized wireless capabilities, into Controlled Access Areas (CAAs) in order to prevent adversaries from using wireless signals to collect and/or transmit classified information.
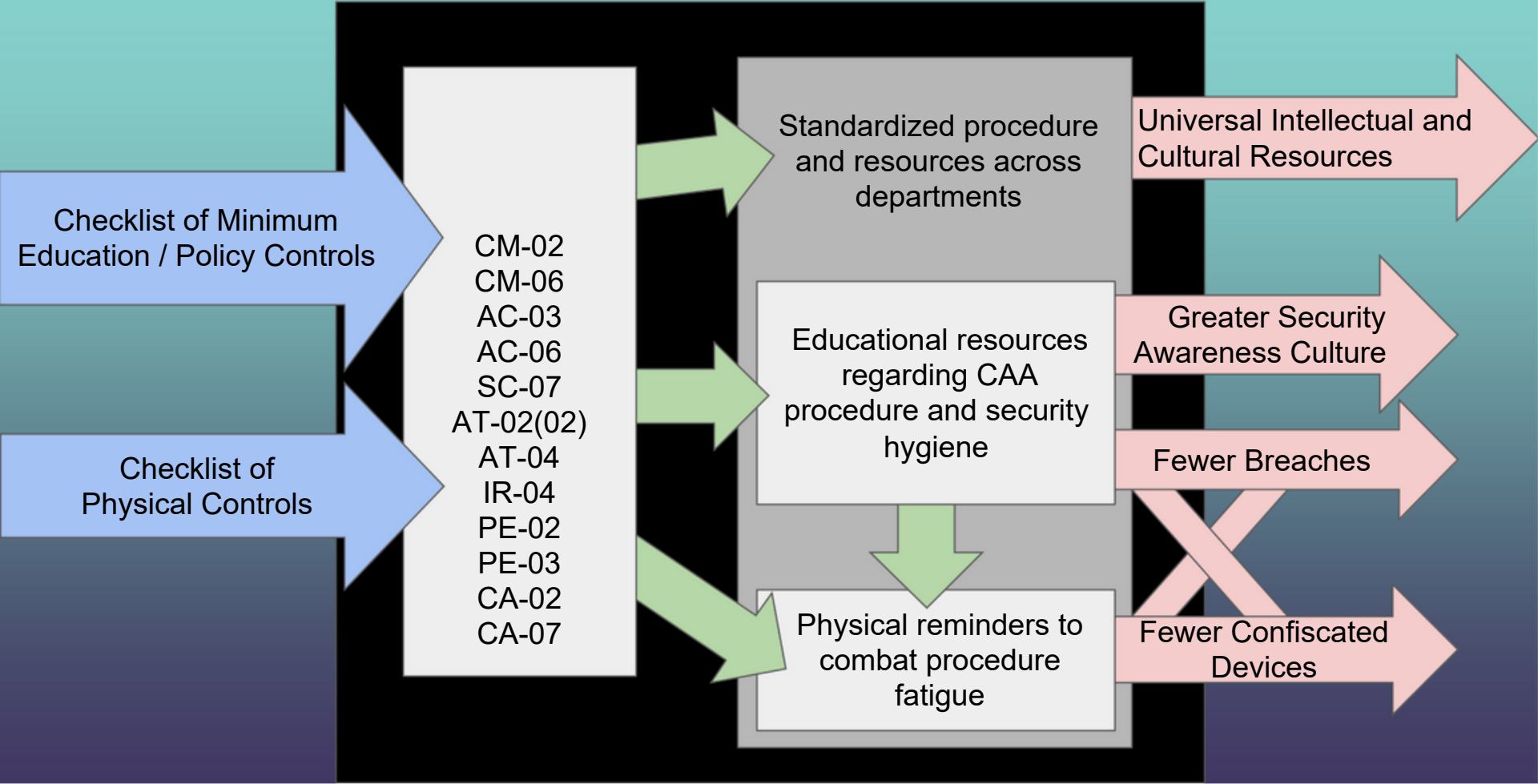
Final Problem Statement

Stop people from inadvertently bringing in smart devices in Controlled Access Areas (CAAs) by **establishing an umbrella standard for both security education and physical controls using standardized NIST 800-53 protocols and Intelligence Community Directives (ICDs)**
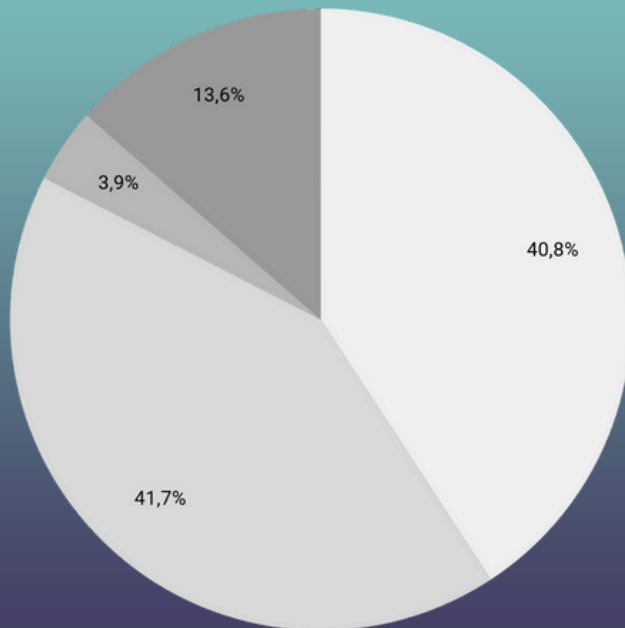
# First Minimal Viable Product

Education →

Policy Changes →

Physical Controls →

CAA Security;
- Detection
- **Prevention via education**
- Mitigation

→ Less policy violation incidents

→ Less confiscated devices

→ Greater security awareness culture

Final Minimal Viable Product

Checklist of Minimum Education / Policy Controls

Checklist of Physical Controls

CM-02
CM-06
AC-03
AC-06
SC-07
AT-02(02)
AT-04
IR-04
PE-02
PE-03
CA-02
CA-07

Standardized procedure and resources across departments

Educational resources regarding CAA procedure and security hygiene

Physical reminders to combat procedure fatigue

Universal Intellectual and Cultural Resources

Greater Security Awareness Culture

Fewer Breaches

Fewer Confiscated Devices

Interview Breakdown

Total Interviews: 103

- Academic
- State Department
- Department of Defense
- Private Sector

13,6%

3,9%

40,8%

41,7%

Interview Archetype Breakdown
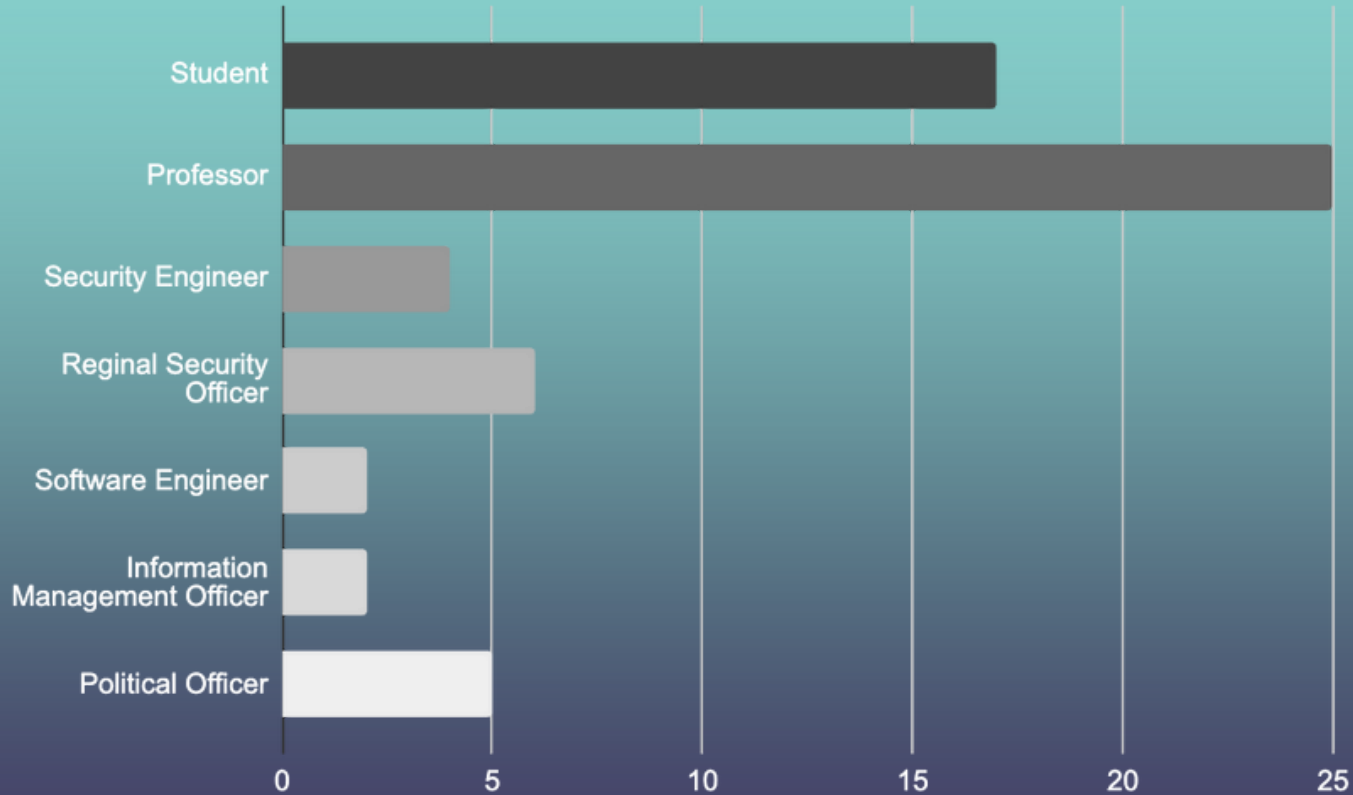
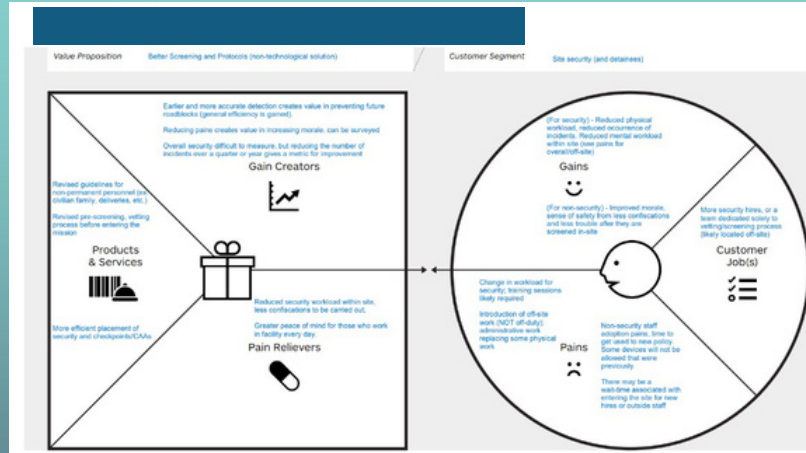# Project Timeline

Weeks 1-5

Total Interview: 21
Days Left: 70

Weeks 1-5

- Meeting with our sponsors to gain a better understanding of our problem statement

- Discovery Interviews
  - Interviewed with educators, fellow students, intelligence community, and security engineers

Weeks 1-5 Interviews

Week 3 Pivot: Stop people from inadvertently bringing in smart devices in Controlled Access Areas (CAAs) and how we can make using smart devices for work purposes easier

Weeks 1-5 Mission Model Canvas

The Mission Model Canvas

Mission/Problem Description: ___   Designed by: ___   Date: ___   Version: ___

Key Partners

Security technology providers for smart device detectors and wearable signal blockers

Security experts and trained for briefings and trainings

Technology vendors for automate reminder systems and AI powered security cameras

Problem statement sponsors

Key Activities

Development and deployment of smart device detectors and blockers

Establishment of personal device lockers

Training and culture shift

Personnel reminder / alert systems

Conducting surprise device audits

Implementation of integrated security camera analysis

Key Resources

Education

Communication systems for personalized alerts

Feedback mechanisms for system improvement

Training materials and instructors

Automatic reminder systems

Physical controls

Wearable signal blockers

Security cameras

Smart device detectors

Faraday cage

Personal device lockers

Value Propositions

Enhanced security by preventing the inadvertent entry of smart devices into controlled access areas

Increased awareness and vigilance among security personnel

Peace of mind for employees

Avoidance of legal issues with solutions

Avoidance of security breaches

Avoidance of unnecessary delays and unwanted confiscations

Buy-in & Support

Local embassy security officers

Local embassy management

Buy in if we achieve both traffic flow efficiency and increase security

Department of state bureau of diplomatic security

Deployment

Pilot test at tri-mission Brussels

Department of defense attaché

Full-scale rollout across multiple us embassies and consulates

Beneficiaries

Marine Security guards

Public diplomacy

Office of legal attaché

Federal aviation federation

Regional security officer

Joint administrative service

Office of defense attaché

Department of homeland security

Ambassadors

Foreign agricultures service

Mission Budget/Cost

Costs associated with technological implementation

Expenses for training sessions and materials

Maintenance and operational costs for automated reminders and security cameras

Personnel costs for surprise audits and system monitoring

Mission Achievement/Impact Factors

Number of CAAs with implemented solutions

Percentage reduction in security breaches related to smart devices

Frequency and effectiveness of trainings

Maintenance and system performance metrics

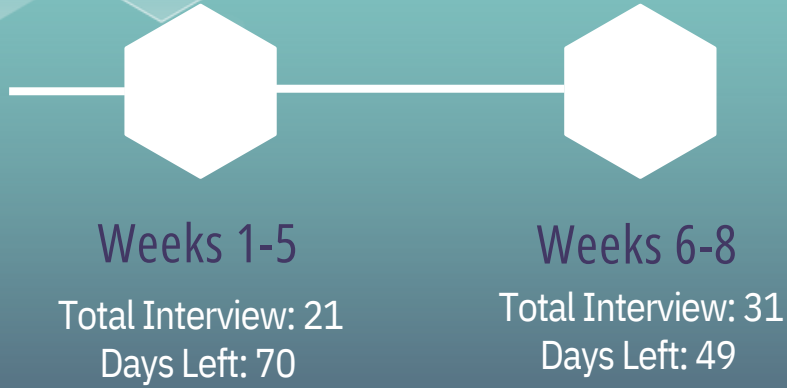Feedback and satisfaction ratings from security personnel and stakeholders

Strategyzer
strategyzer.com

Project Timeline

Weeks 1-5

Total Interview: 21
Days Left: 70

Weeks 6-8
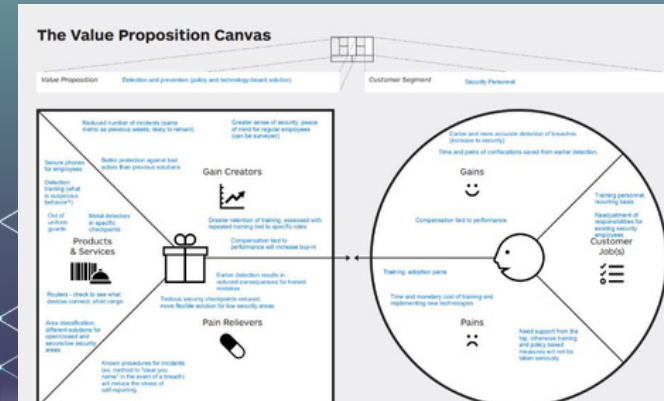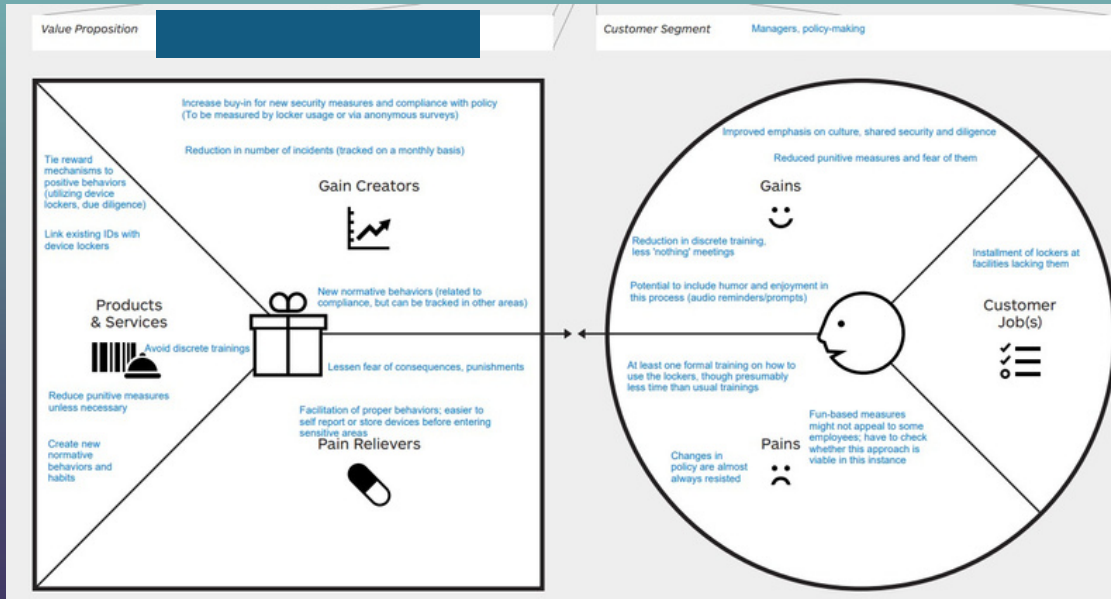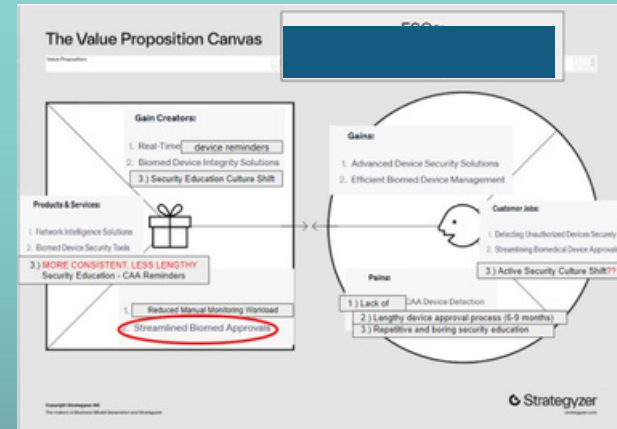
Total Interview: 31
Days Left: 49

Weeks 6-8

- Focused on finding ways to make using smart devices easier in CAA's

- Shift towards an educational solution

- Increased emphasis on policy

- Increased awareness of the cultural element

Weeks 6-8 Interviews

Security Personnel: Solution categorization, focal points of training

Management: OB, cultural element

Weeks 6-8 Mission Model Canvas

The Mission Model Canvas

Mission/Problem Description:	Designed by:	Date:	Version:

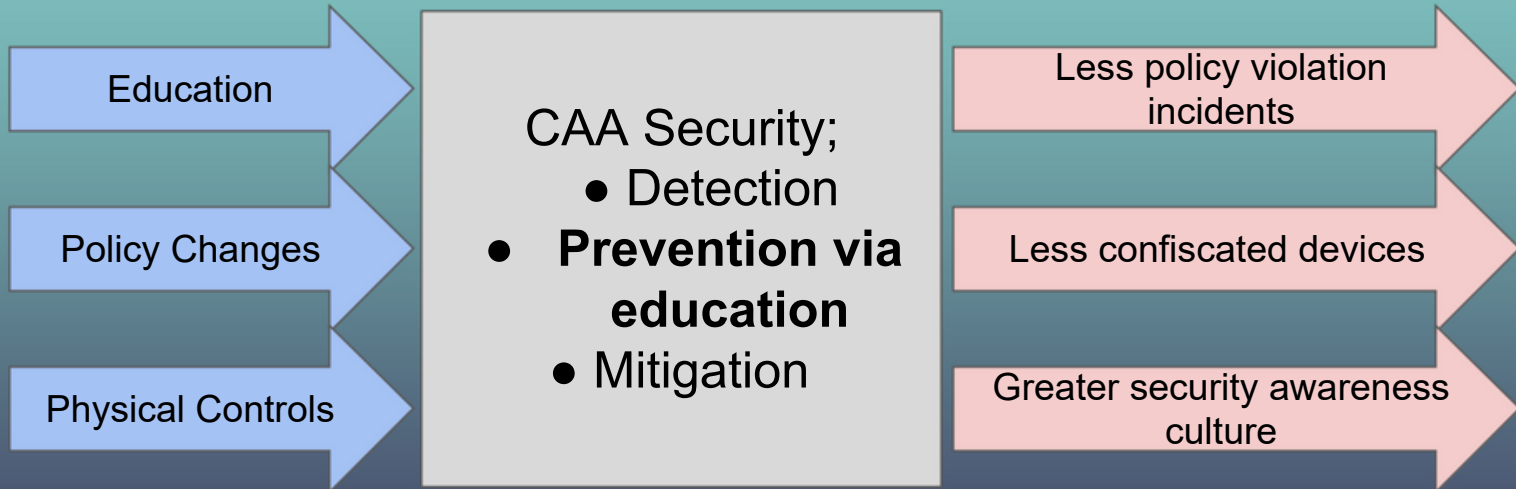| Key Partners	Key Activities	Value Propositions	Buy-in & Support	Beneficiaries
Security experts and trained for briefing Security technology providers for smart device detectors and signal blockers Sponsors	AT-1: training and culture shift SI-5: personal reminder/ alert IA-3: device smart detectors PE-7: personal device lockers	Increased awareness and vigilance among security personal Avoidance of legal issues Enhanced security by preventing entry of smart devices in CAA Avoidance of unnecessary delays and confiscations Avoidance of security breaches Peace of mind for employees	Local embassy security officers Local embassy management Department of state bureau of diplomatic security	Marine Security Guards Office of Legal Attaché Regional Security Officer Department of Homeland Security Office of Defense Attaché Public Diplomacy Intelligence Community
	Key Resources System for alerts Feedback for system improvement Training materials and instructor Wearable signal blockers Smart device detectors Faraday cage Personal device lockers		**Deployment** Pilot test at Tri-Mission Brussels Department of Defense Attaché Full-scale rollout across multiple embassies and consulates	

Mission Budget/Cost	Mission Achievement/Impact Factors
Cost associated with technological implementation Expenses for training sessions and materials Maintenance and operational cost for personal reminders Cost for audit and monitoring	CAA with implemented solution Percentage reduction in security breaches related to smart devices Frequency and effectiveness of trainings Maintenance and system performance metrics Feedback and satisfaction ratings from security personnel and stakeholders

Strategyzer
strategyzer.com

Week 6 - First Minimal Viable Product

Education →

Policy Changes →

Physical Controls →

CAA Security;
● Detection
● **Prevention via education**
● Mitigation

→ Less policy violation incidents

→ Less confiscated devices

→ Greater security awareness culture

Week 7 - Second Minimal Viable Product
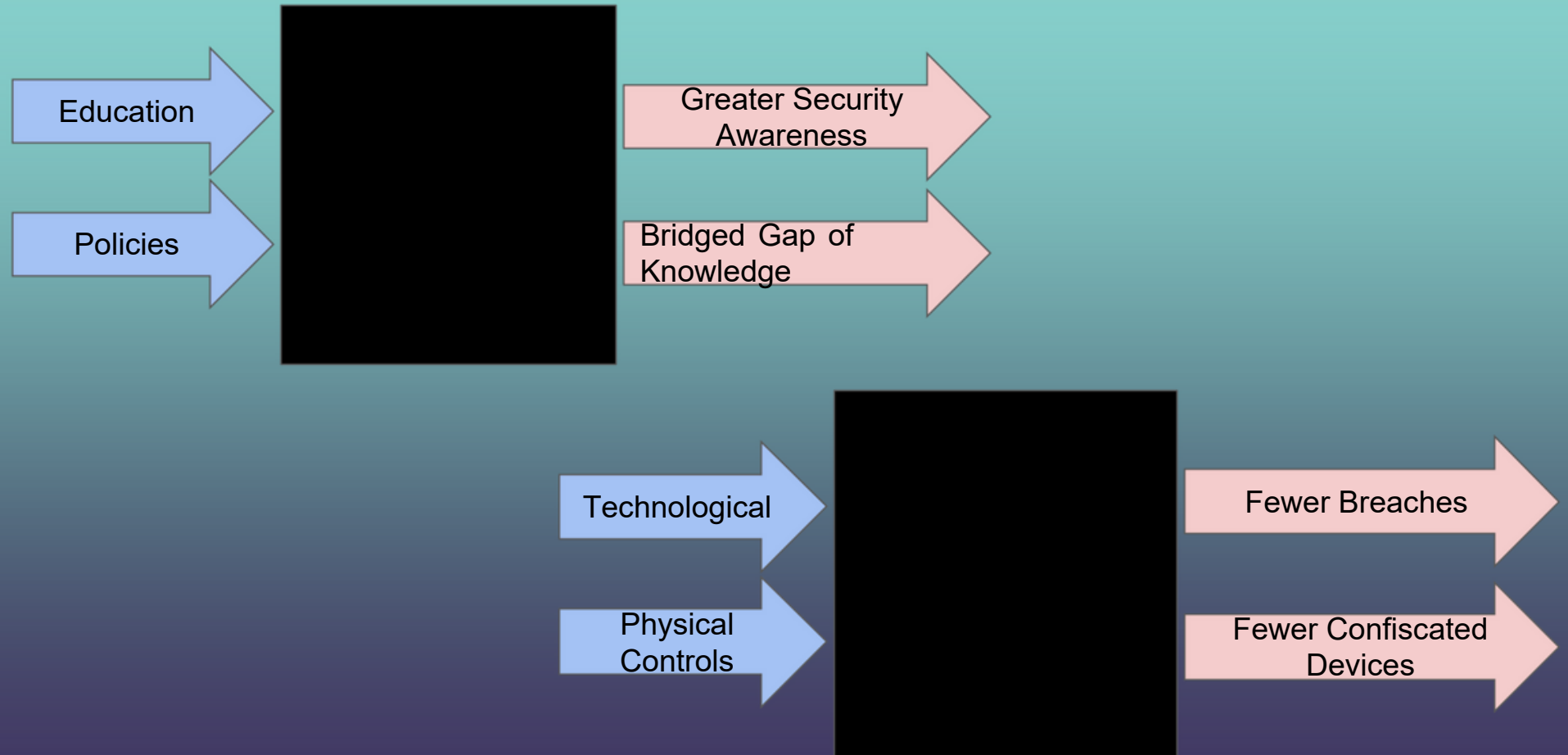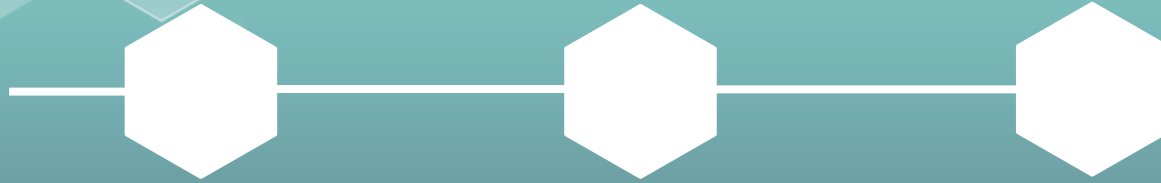
Education →

Policies →

Greater Security Awareness →

Bridged Gap of Knowledge →

Technological →

Physical Controls →

Fewer Breaches →

Fewer Confiscated Devices →

Project Timeline

Weeks 1-5

Total Interview: 21
Days Left: 70

Weeks 6-8

Total Interview: 31
Days Left: 49

Weeks 9-11

Total Interview: 49
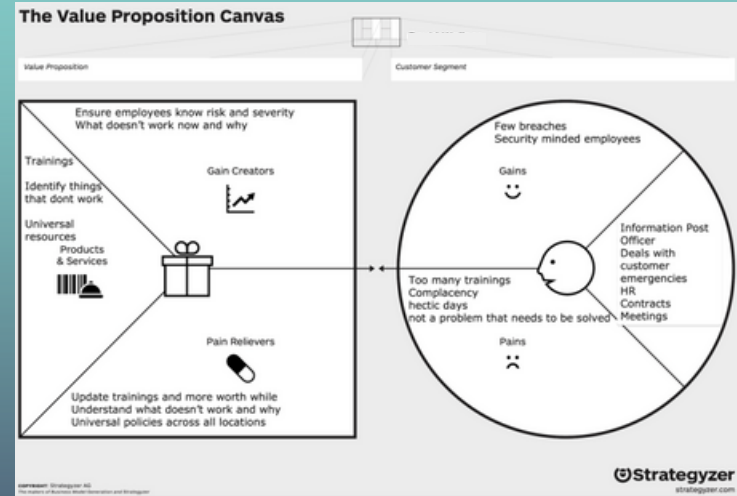Days Left: 28

Weeks 9-11

- How can we establish a security culture?

- Changed the entire focus of our project

   ○Shifted to finding a standardization across all locations

Weeks 9-11 Interviews

Information Post Officer

- Emphasized that they do not need more training

- Already had a lot of different solutions in place

The Value Proposition Canvas

Value Proposition | Customer Segment

Ensure employees know risk and severity
What doesn't work now and why

Trainings

Identify things that dont work

Universal resources
Products & Services

Gain Creators

Update trainings and more worth while
Understand what doesn't work and why
Universal policies across all locations

Pain Relievers

Few breaches
Security minded employees

Gains

Too many trainings
Complacency
hectic days
not a problem that needs to be solved

Information Post Officer
Deals with customer emergencies
HR
Contracts
Meetings

Pains

Strategyzer
strategyzer.com

Weeks 9-11 Mission Model Canvas

The Mission Model Canvas

Mission/Problem Description:

Designed by:

Date:

Version:

Key Partners

Security experts and trained for briefing

Security technology providers for smart device detectors and signal blockers

Intelligence Community

Joshua Ellwein

Jose Moreno

Key Activities

AT-1: Training and culture shift

SI-5: Personal reminder / alerts

IA-3: Device smart detectors

PE-7: Personal device lockers

Unified Training material

Key Resources

- System for alerts
- Feedback for system improvements
- Training materials and instructor
- Wearable signal blockers
- Smart device detectors
- Faraday Cage
- Personal device lockers

Value Propositions

Increased awareness and vigilance among security personnel

Avoidance of legal issues

Enhanced security by preventing entry of smart devices in CAA

Avoidance of unnecessary delays and confiscations

Avoidance of Security Breaches

Peace of mind for employees

Buy-in & Support

Local Embassy Security Officers

Local Embassy Management

Department of State Bureau of Diplomatic Security

Deployment

Pilot test at Tri-Mission Brussels

Department of Defense Attache

Full-scale rollout across multiple embassies and conulates

Beneficiaries

Security Engineering Officer

Division Director

Security Technician Specialist

Regional Security Officer

Information Management Officer

Information Systems Officer

Counselor for Political and Economic Affairs

Political Officer

Economic Officer

Marine Security Guards

Mission Budget/Cost

Cost associated with technological implementation

expenses for training sessions and materials

Maintenance and operation cost for personal reminders

Cost for audit and monitoring

Mission Achievement/Impact Factors

Percentage reduction in security breaches related to smart devices
Frequency and effectiveness of trainings
Maintenance and system performance metrics
Feedback and satisfaction ratings from security personnel and stakeholders

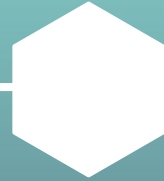Strategyzer

strategyzer.com

Project Timeline

Weeks 1-5

Total Interview: 21
Days Left: 70

Weeks 6-8

Total Interview: 31
Days Left: 49

Weeks 9-11

Total Interview: 49
Days Left: 28

Weeks 12-15

Total Interview: 103
Days Left: 0

Weeks 12-15

- Looked into physical controls using standardized NIST 800-53 protocols and Intelligence Community Directives (ICDs)
- Site Visit to Ottawa Embassy
  - Group discussion regarding challenges when using CAAs
  - Especially regarding the differences in CAA layout between embassies and consulate
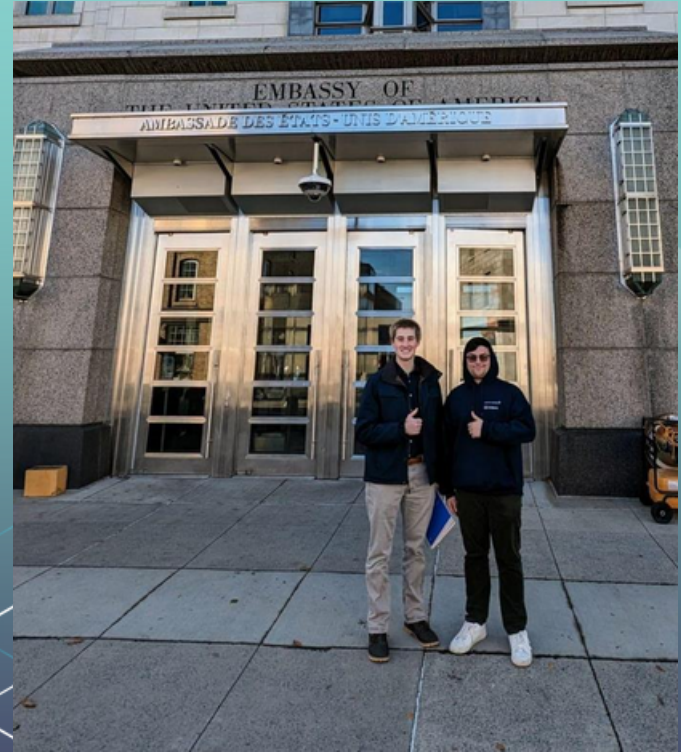
Weeks 12-15 Interviews

- Lots of valuable group discussion and "on-the-ground" information gathering
  ◯ Embassy layout differences
    ◯ NEC (New Embassy Compounds) are structured differently than embassies made prior to the Nairobi and Dar es Salaam attacks
- Back to back in-person interviews lets us build discussions off of each other

Weeks 12-15 Mission Model Canvas

The Mission Model Canvas

Mission/Problem Description:	Designed by:	Date:	Version:

Key Partners 🔗

Security experts and trained for briefing

Security technology providers for smart device detectors and signal blockers
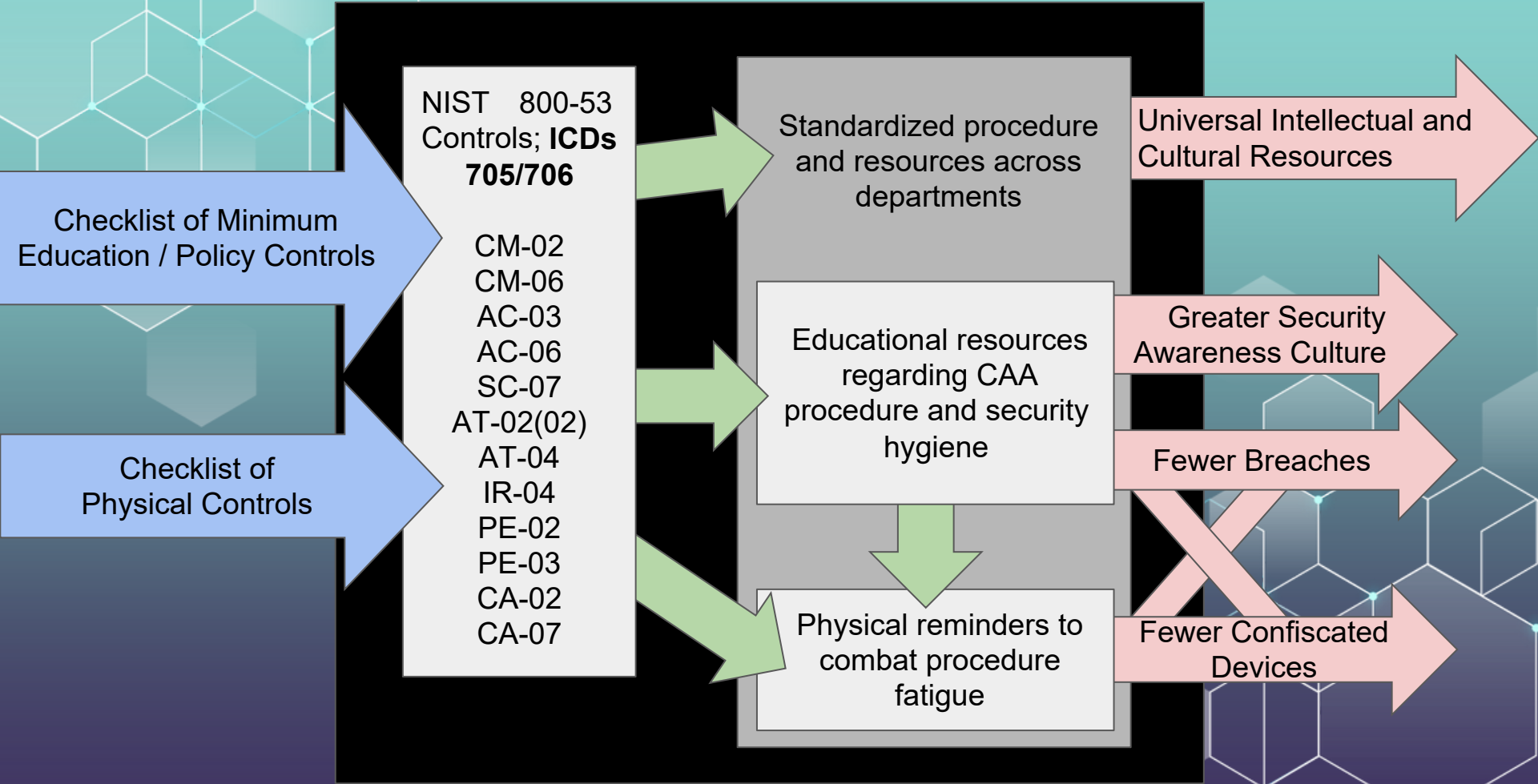
Intelligence Community

Joshua Ellwein

Jose Moreno

Jason Hewkin (Ottawa)

Key Activities ✓

AT-1: Training and culture shift

SI-5: Personal reminder / alerts

IA-3: Device smart detectors

PE-7: Personal device lockers

Unified Training material

Key Resources 👷

- System for alerts
- Feedback for system improvements
- Training materials and instructor
- Wearable signal blockers
- Smart device detectors
- Personal device lockers
- Rotating auditory prompts

Value Propositions 🎁

Increased awareness and vigilance among security personnel

Avoidance of legal issues

Enhanced security by preventing entry of smart devices in CAA

Avoidance of unnecessary delays and confiscations

Avoidance of Security Breaches

Peace of mind for employees

Buy-in & Support ♥

Local Embassy Security Officers

Local Embassy Management

Department of State Bureau of Diplomatic Security

Deployment 🚚

Pilot test at Tri-Mission Brussels

Department of Defense Attache

Full-scale rollout across multiple embassies and conulates

Beneficiaries 😶

Security Engineering Officer

Division Director

Security Technician Specialist

Regional Security Officer

Information Management Officer

Information Systems Officer

Counselor for Political and Economic Affairs

Political Officer

Economic Officer

Marine Security Guards

Mission Budget/Cost 🏷

total cost = physical control procurement + training cost + auditing + incident response

Mission Achievement/Impact Factors 🏔

Percentage reduction in security breaches related to smart devices (<213,000)
Frequency and effectiveness of trainings
Maintenance and system performance metrics
Feedback and satisfaction ratings from security personnel and stakeholders

Ⓢtrategyzer
strategyzer.com

Final Minimal Viable Product

Nist Controls

CM-06
Configuration Settings

AC-06
Least Privilege

AT-02(02)
Security Training and Awareness

IR-04
Incident Handling

CM-02
Configuration Management Policy and Procedures

AC-03
Access Enforcement

SC-07
Boundary Protection

AT-04
Security Training and Awareness Records

PE-02
Physical Access Authorizations

PE-03
Physical Access Controls

CA-02
Security Assessment and Authorization
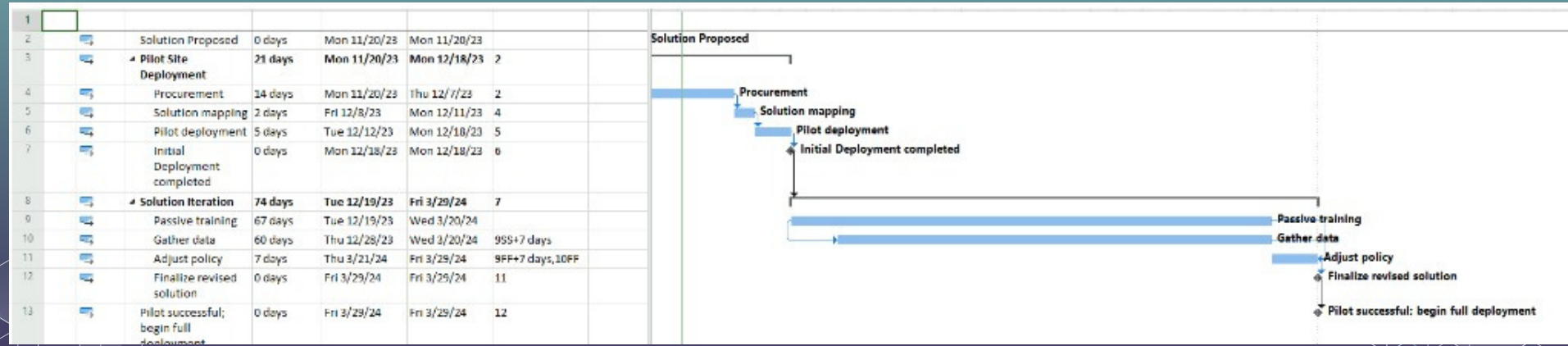
CA-07
Continuous Monitoring

Deployment

- **Pilot Deployment**
- **Information gathering, adjustments and**
- **iteration Full deployment**

Special Thanks

Joshua Ellwein
Jose Moreno

Problem
Sponsors

Jason Hewkin

ESO -Ottawa
Embassy

Joe   Calamari
Lillian
Herrera
Industry Mentors

Jim   Santa
Suvam Barui

Course
Managers

Questions?