



Odin Agenda Friday March 11th 2016

Time	Topic	Location / Attendees	Speaker
9:00am – 9:30am	Logistics, Program Introduction	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
9:30am – 10:10am	IARPA Overview	NOAA Open to Everyone	Dr. Stacey Dixon Deputy Director
10:10am – 10:20am	Break		
10:20am – 11:00am	Odin Technical Overview	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
11:00am – 11:30am	Odin BAA Overview	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
11:30am – 12:00pm	Doing Business with IARPA	NOAA Open to Everyone	IARPA Acquisitions
12:00pm – 12:30pm	Q&A Session	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
12:30pm – 1:00pm	Lunch – on your own		
1:00pm – 3:00pm	Poster Session and Teaming Discussions	NOAA No Government	Attendees
1:30pm – 2:00 pm	Check In MS2	MS2	Attendees
2:00 pm – 4:00 pm	Red Team	MS2 Minimum SECRET Clearance	Dr. Chris Boehnen Program Manager
4:00 pm – 5:00 pm	Red Team Teaming Discussions	MS2 No Government SECRET	Attendees

NOAA address is 5830 University Research Ct, College Park MD 20740

MS2 address is 5850 University Research Ct, Riverdale Park MD 20737

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE



(U) Odin: Biometric Presentation Attack Detection

Chris Boehnen Ph.D.
Senior Program Manager Office of Smart Collections



Disclaimer

- This Proposers' Day Conference is provided solely for information and planning purposes
- The Proposers' Day Conference does not constitute a formal solicitation for proposals or proposal abstracts
- Nothing said at Proposers' Day changes the requirements set forth in a Broad Agency Announcement (BAA)
 - IARPA does not guarantee the release or timeline of a BAA, everything here is notional



Proposer's Day Goals

- Familiarize participants with IARPA's interest in research in Presentation Attack Detection (PAD)
- Familiarize participants with IARPA's mission and how to do business with IARPA
- Provide answers to participants' questions
 - This is your chance to alter the course of events
- Foster discussion of synergistic capabilities among potential program participants, i.e., facilitate teaming
 - Take a chance – someone might have a missing piece of your puzzle



Important Points

- Proposer's Day slides will be posted on iarpa.gov
- Please save questions for the end, write on notecards
- Posters are available for browsing during break/lunch
- Government will not be present during the poster/teaming session
- Discussions with PM allowed until BAA release
 - Once BAA is published, questions can only be submitted and answered in writing via the BAA guidance
- Name/email list of Proposer's Day participants provided to the group **with your permission**



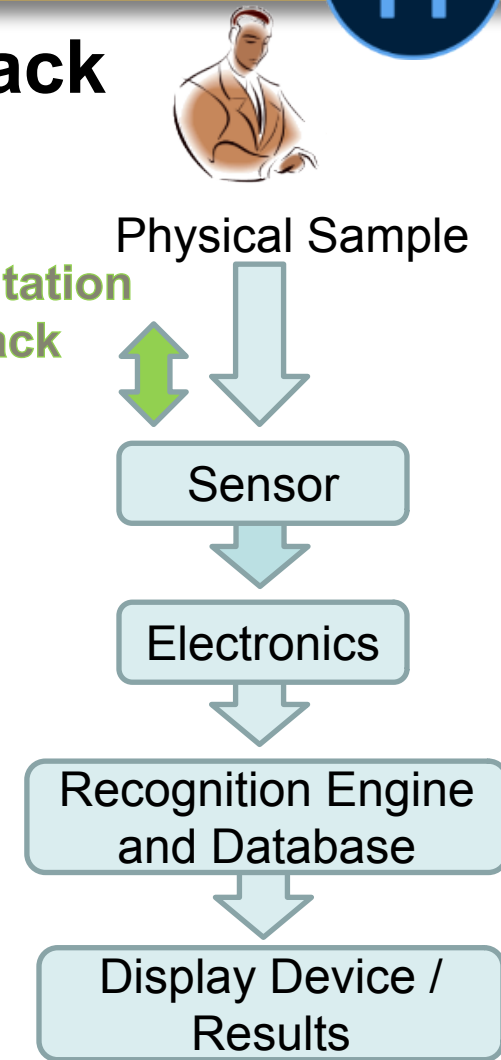
Odin Program Introduction

Biometric Presentation Attack

- A biometric Presentation Attack (PA) is a method which inhibits the intended operation of a biometric capture system interfering with the recording of the true sample/identity, ultimately preventing the subject from being correctly identified
 - Biometric spoofing is common analogous term
 - This is typically accomplished utilizing a prosthetic



Presentation
Attack





The Problem: Biometric collection systems are easily fooled

State of the Art

- Most deployed systems have no Presentation Attack Detection (PAD) capabilities, advanced systems are barely able to detect limited 'static' representations such as a piece of paper
- All systems are 'trained' to find known types of Presentation Attacks (PA)
- Mitigates the biometric collection system vulnerabilities with a human security presence to ensure integrity of the process

Gaps in Current Technology

- Sensor hardware captures limited information pertinent to PAD
- No intelligence in current systems to identify 'unknown' PAs

What We Need

- More robust information on a biometric sample to identify PAs
- An 'intelligent' approach that can identify unknown presentation attacks based on knowledge of what a true sample should look like



The Solution: Odin

Program Goal

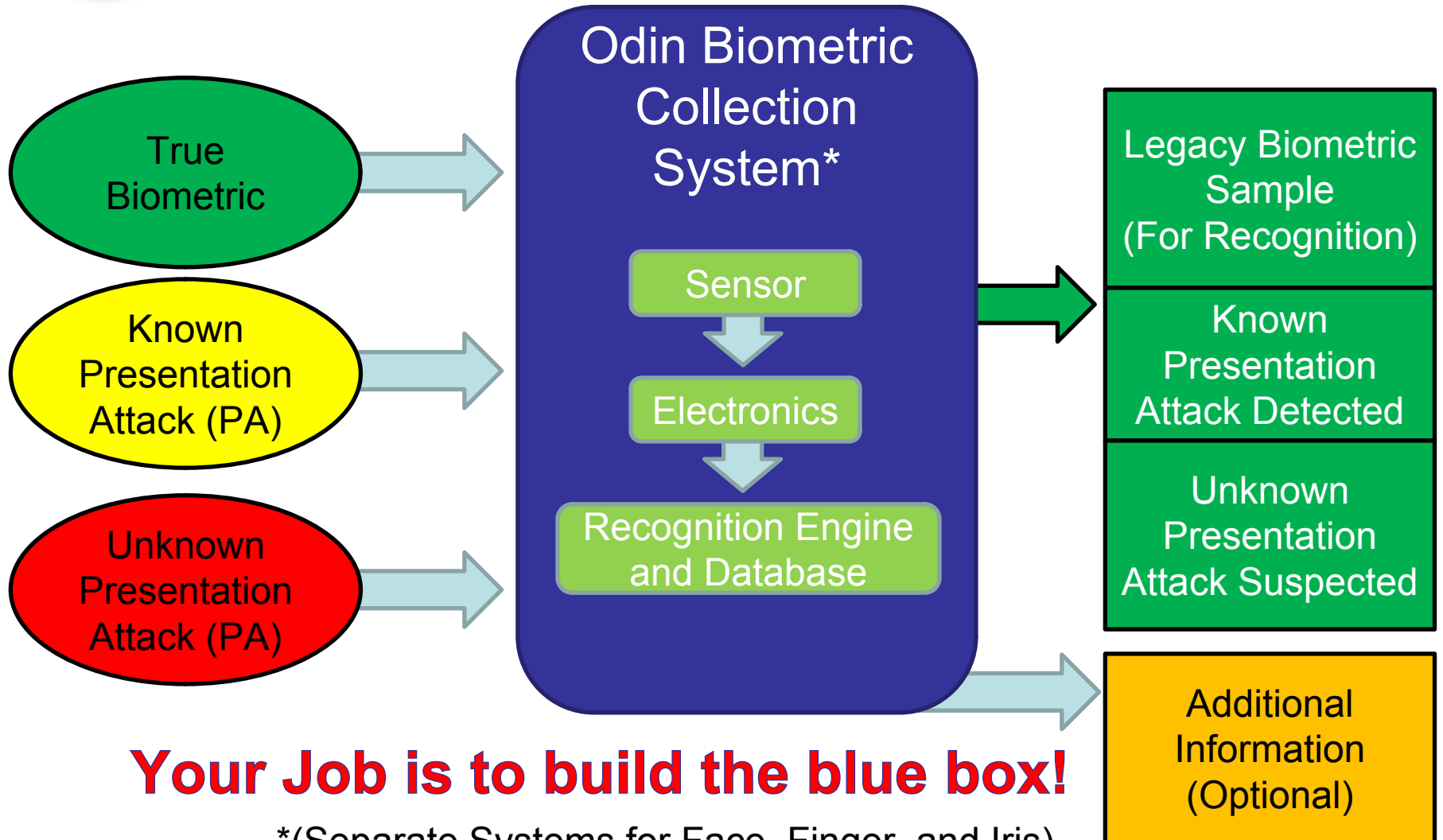
Identify known and unknown presentation attack's within a biometric collection system

Biometric Modalities of Interest

- Face
- Finger
- Iris

System Requirements

- Must be able to provide biometric recognition as good or better than the existing state of the art
- Biometric comparison with existing 'legacy' systems and datasets
- Must be operationally relevant with respect to factors such as
 - Capture time
 - Cost





















Your Job is to build the blue box!

*(Separate Systems for Face, Finger, and Iris)



Biometric Collection Use Cases & Priorities

	PA False Alarm Rate 	PA True Detect Rate 	Cost (\$)	Time	Biometric Recognition 
Border / Travel Crossing	Small FAR 			Fast 	Highly Accurate 
Visa Applications			Expensive 	Long 	Highly Accurate 
HS Facility Access	Higher FAR	Higher TDR 	Expensive	Long 	Highly Accurate
HS Cyber Authentication		Higher TDR		Fast	
LS Facility Access					
LS Cyber Authentication		Lower TDR	Cheap	Fast	Low Accuracy

HS = High Security
LS = Low Security

Note: This is not an official government position, but an example to demonstrate diverse use cases



IARPA Introduction

Dr. Stacey Dixon

Deputy Director IARPA



Odin Agenda Friday March 11th 2016

Time	Topic	Location / Attendees	Speaker
9:00am – 9:30am	Logistics, Program Introduction	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
9:30am – 10:10am	IARPA Overview	NOAA Open to Everyone	Dr. Stacey Dixon Deputy Director
10:10am – 10:20am	Break		
10:20am – 11:00am	Odin Technical Overview	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
11:00am – 11:30am	Odin BAA Overview	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
11:30am – 12:00pm	Doing Business with IARPA	NOAA Open to Everyone	IARPA Acquisitions
12:00pm – 12:30pm	Q&A Session	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
12:30pm – 1:00pm	Lunch – on your own		
1:00pm – 3:00pm	Poster Session and Teaming Discussions	NOAA No Government	Attendees
1:30pm – 2:00 pm	Check In MS2	MS2	Attendees
2:00 pm – 4:00 pm	Red Team	MS2 Minimum SECRET Clearance	Dr. Chris Boehnen Program Manager
4:00 pm – 5:00 pm	Red Team Teaming Discussions	MS2 No Government SECRET	Attendees

NOAA address is 5830 University Research Ct, College Park MD 20740

MS2 address is 5850 University Research Ct, Riverdale Park MD 20737



Odin Technical Overview



Odin Goal

- The goal of Program Odin is to identify known and unknown Presentation Attacks (PA) in a biometric collection system
 - Input: A live human
 - Output:
 - Known, unknown PA status
 - E.g. Binary value
 - Biometric sample for recognition
 - E.g. Electronic Biometric Template (EBT)
 - Interoperable with legacy systems, biometric recognition/identification/verification performance at or above state of the art
 - Must be operationally viable (more on this later)



How is it Done Today?

Approaches	Examples
Liveness detection	Oxygen hemoglobin sensors, heartbeat, pupil dilation, and more
Intrinsic Properties	Multi-layer fingerprint, color texture, electrical resistance, biometric specific features such as iris texture analysis, and more
Artificial Indicators	Dot matrix pattern detection, spectral examination, and more
Human Personnel	Security Guards

Sensor Technology Examples

- Optical
- Multi-Spectral
- Electrical
- Ultrasound
- Structured Light
- LIDAR
- Stereo
- Optical Coherence Tomography



How is Odin Different

- Sensors
 - Capture multi-modal information that may include some of the following (but is not limited to just these either)
 - **Textural** (2D Color)
 - **Optical** (Spectral)
 - **Structural** (3D)
 - **Temporal** (Motion)
 - May utilize commercial off the shelf, state of the art, or research/develop a new sensor
- Analysis of Information
 - Identify unknown presentation attacks by learning a corpus of known biometric data
 - Utilize single class/outlier detection instead of looking for characteristics of known presentation attacks

IARPA/Odin is not limiting performers to this approach!



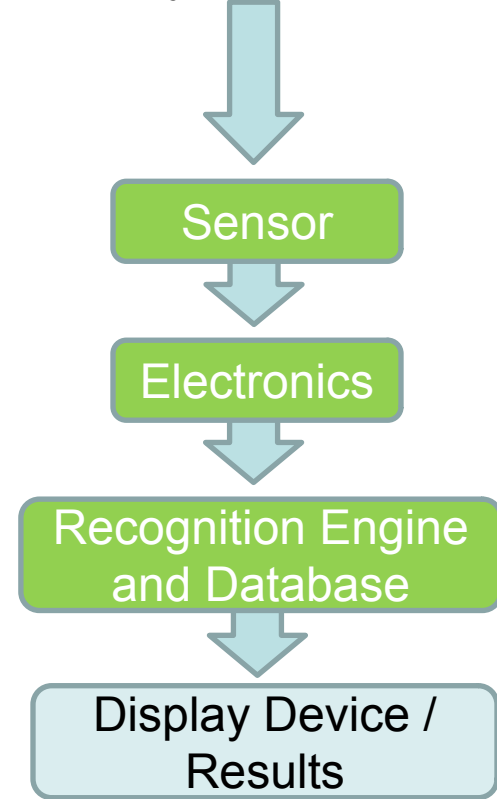
Odin Research Scope

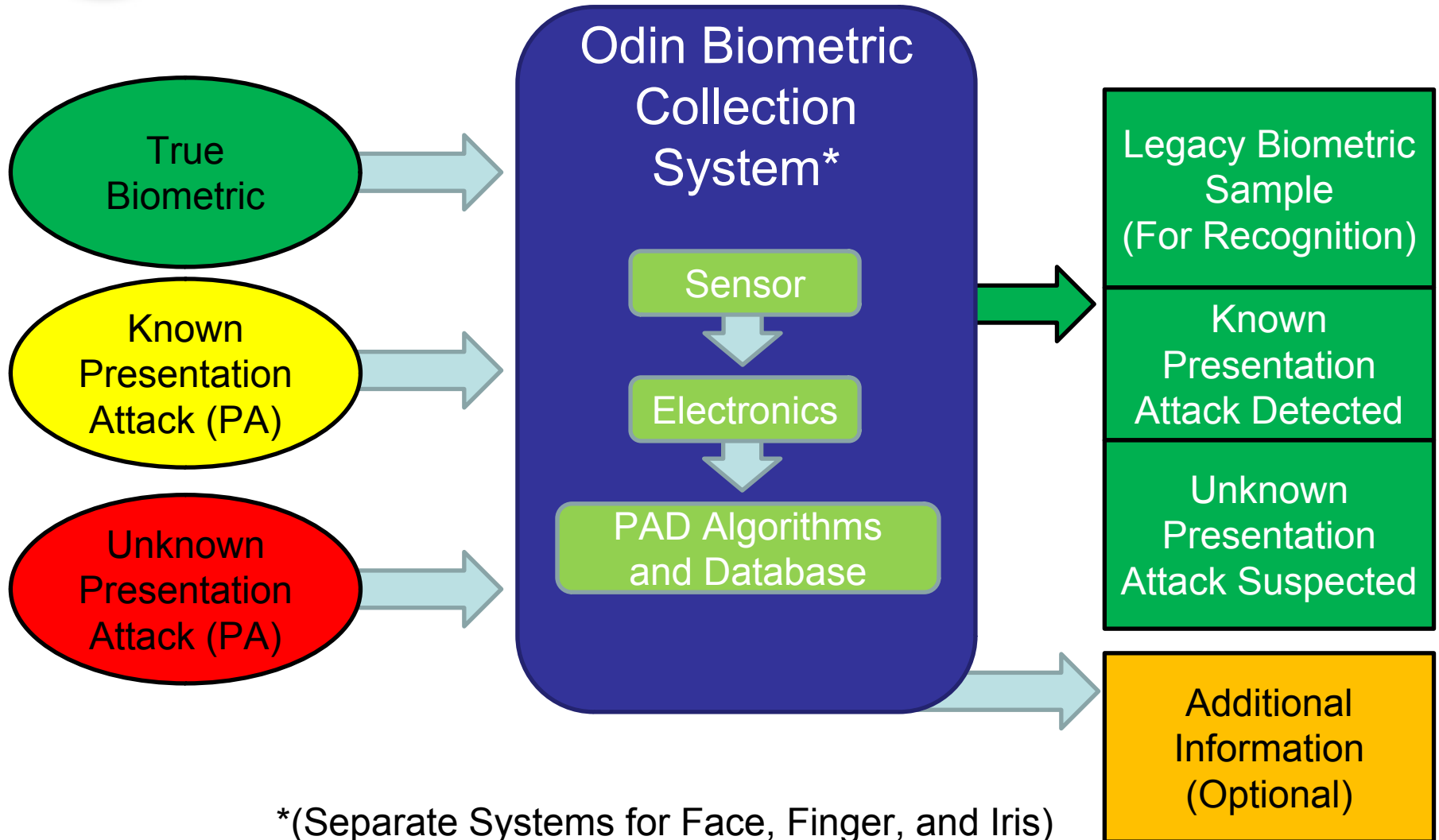
- In Scope Research Examples
 - Sensor hardware
 - Analysis algorithms
 - Database
- Out Of Scope Examples
 - IC chip security
 - Traditional digital cyber security
 - Database encryption
 - Security personnel operational training

Biometric Collection System



Physical Sample





*(Separate Systems for Face, Finger, and Iris)



Odin Biometric Recognition Modalities

- In Scope (live capture)
 - Fingerprint
 - Face
 - Iris
- Out of Scope (Everything else)
 - DNA
 - Voice
 - Gait
 - Ear
 - Latent Fingerprint
 - Digital File (including digital manipulations)
 - Etc.



Odin Modalities

- Do not have to make “one system to rule them all”, can make either
 - 1 system tailored for each modality (3 systems total)
 - 1 system for every modality (1 system total)

Face, finger & iris biometric collection system

or

Face biometric collection system

Finger biometric collection system

Iris biometric collection system



Odin data capture

- Can examine other parts of the body for PAD detection, but has to do it in a way that ensures all data is from the same person
 - If you can capture the ear while capturing the face and want to use both for PAD that's acceptable
 - E.g. perriocular with iris, face with iris, iris with face, and more
 - If you build a PAD fingerprint sensor and want to enhance it with a separate PAD ear system that's probably not ok
 - E.g. finger with toe, finger with face, finger with ear, and more probably not ok

Program Odin Naming and Structure

- **Odin T&E**
 - Norse Mythology: Revered Norse God
 - Test Thor's ability to detect presentation attacks
- **Thor BAA**
 - Norse Mythology: Son of Odin, brings peace and justice
 - Ability to detect unknown and known presentation attacks
- **Loki BAA**
 - Norse Mythology: Trickster, known for causing chaos
 - Goal is to red team Thor assisting T&E





Security / Classification

- Thor
 - Unclassified, foreign participants allowed
 - Will be provided with presentation attacks to test by USG Odin T&E team
 - Not permitted to develop 'new' presentation attack methods
 - Your information may be shared with selected Loki performers
- Loki
 - Classified performer base
 - Because the goal of Odin is to identify unknown vulnerabilities, Thor performers (regardless of possession of a clearance) will not be kept apprised of Loki specifics.
 - Due to the security sensitivity of vulnerabilities, all discussions on Loki will be reserved for the afternoon session
- May only be a performer on one team



Presentation Attacks

- Odin T&E will provide PAs to Thor
 - May include physical samples
 - May include technique for making a PA that Thor performers can replicate
- Thor Performers may
 - Request permission for Thor teams to replicate known PAs from the open community (Government approval required to proceed)
- Thor Performers may not
 - Develop and manufacture new PAs not already known to the open community or publish on possible PA approaches not already known to the open community
- While IARPA cannot, and is not attempting to, control what is done by anyone outside of the Thor program, these restrictions will apply to Thor funds. Thor funds may not be used in conjunction with other sources to circumvent this restriction.



Testing and Results

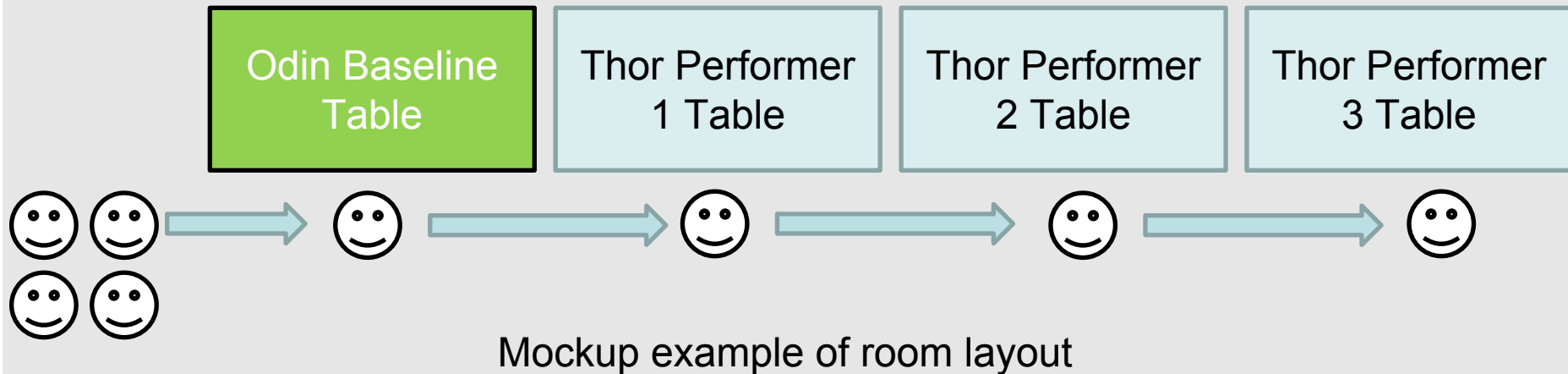
- A single test will consist of several hundred live human subjects with and without presentation attacks against Thor systems
 - Performer Self Reported Tests (Results Shared)
 - **Government Controlled Tests (Results Shared)**
 - Performer participation for provided presentation attacks
 - Held at common physical location for all performers
 - **Private USG Testing (Results Not Shared)**
 - Performer not present for held back presentation attacks





Odin Government Controlled Test

- Same person will visit each station to provide a common subject pool for testing
- Odin T&E will have a baseline to understand current state of the art for PAD and biometric recognition





Performer Self Reported Tests

- PAD Operator: 1 Thor Performer
- PA Operator: 1 Thor Performer
- Presentation Attacks:
 - Provided by Odin T&E to Thor, all known to Thor
 - May include procedure for training with subset of PAs to simulate ‘unknown’ PAs in testing
- Observers: Possible Odin T&E, Others
- Location: Thor Performer

- Results
 - Shared with all

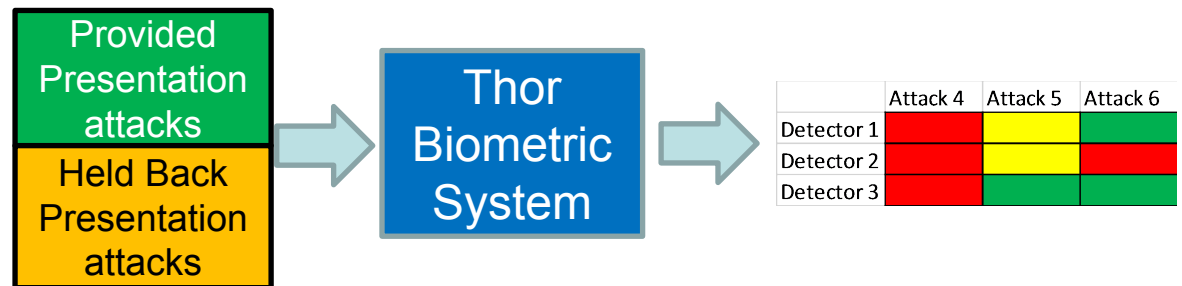




Government Controlled Tests

- PAD Operator: 1 Thor Performer
- PA Operator: Odin T&E
- Presentation Attacks:
 - Some known, some unknown to Thor provided by Odin T&E
 - May include procedure for training with subset of PAs to simulate ‘unknown’ PAs in testing
- Observers: Odin T&E, Others
- Location: Common USG Location

- Results
 - Shared with all





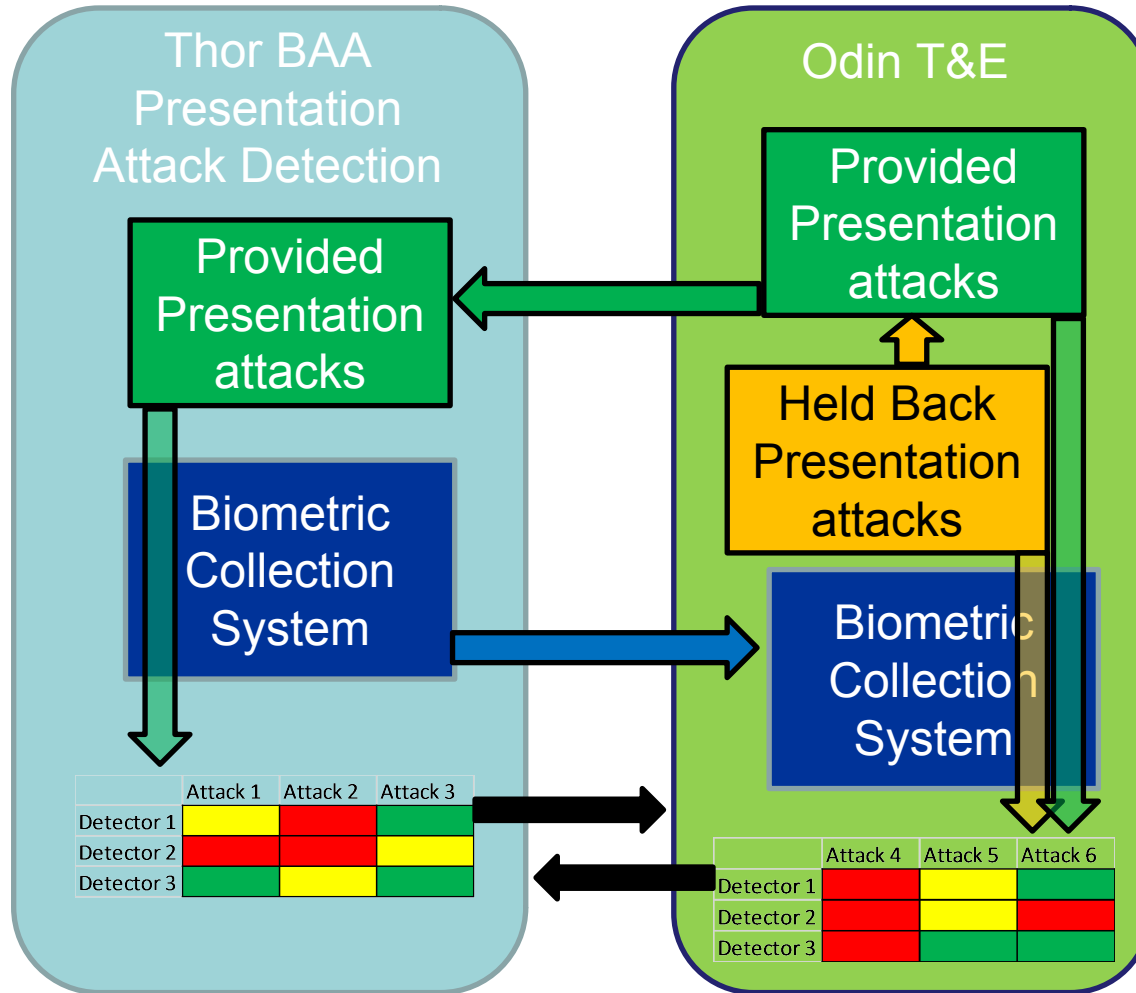
Private USG Testing

- PAD Operator: Odin T&E
- PA Operator: Odin T&E
- Observers: None
- Location: USG
- Results
 - Private





Odin Program Testing Structure





Number of Subjects for Testing

- Notional minimal number of subjects for testing
 - Subject to change
 - Minimal, more is always better

	Phase 1			Phase 2					Phase 3			
	S	S	G	S	S	G	S	G	S	G	S	G
Self or Government Reporting												
Thor Presentation Attack trials	100	200	200	100	200	100	100	200	100	100	500	500
Thor True Attempts	200	300	400	200	400	200	400	500	200	250	750	1000



Metrics and Constraints

- Metrics
 - Measuring progress towards specific technical program goals
 - Focus of the program, want to get as good as possible
- Constraints
 - Has a minimum requirement that must be met
 - Improvements upon the minimum are good, but secondary objectives of the overall program



Constraint: Projected Component Cost

- The cost of similar components for your sensor purchased in bulk today
 - Components for comparison do not need to be a perfect match
 - Using an RGB sensor as a stand in for an expensive multispectral imaging sensor is probably ok if you can argue that at volume the cost of the multispectral imaging sensor would be lower
 - Does not need to include computation resources (e.g. a computer), just the sensor
 - If your approach requires a mass spectrometer, electron microscope, and other expensive laboratory tools it probably can't meet this constraint
 - Cost (\$5,000) is per modality. If you are building one sensor to do all three (face, finger, iris), cost is \$15,000.



Constraint: Temporal Representation

- The amount of time the subject would need to be present to capture the sample in a fielded system
 - If your prototype actually takes less than 30 seconds to capture the sample, you don't need to do anything other than state that
 - If it takes longer than 30 seconds, you need to justify that it could be possible with engineering improvements to speed it up, but that at the prototype stage it isn't worth the effort
 - 3D laser scanner takes a while, but you can argue it could be sped up with further development to satisfy this constraint
 - Requiring an hour worth of data to analyze the heartbeat or facial expressions is not ok



Thor Metric and Constraints

Category	Metric	Odin Goal
PAD	TDR @ FAR 0.2%	97.00%
Category	Constraint	
Biometric Performance	Face Biometric EER	2.00%
	Finger Biometric EER	1.00%
	Iris Biometric EER	0.50%
Operational	Projected Components Cost	\$5,000
	Temporal Representation	30 Seconds

- Metric and Constraints shown are notional and simplified for discussion
 - BAA will spell out more complex test
 - Performers should be able to meet or exceed constraints, but exceeding is a secondary goal to performance for the primary metric
- Values are not a “go/no go” decision point
- Goals shown are for entire program, each phase will have different values

PAD = Presentation Attack Detection, **TDR** = True Detect Rate,
FAR = False Alarm Rate, **EER** = Equal Error Rate



Multi disciplinary Important!

- This isn't really a 'Biometric' program
- Biometric domain expertise is important, but equally important are sensor, computer vision, and machine learning expertise focused on counterfeit/fraud detection in the biometric domain
- Multi disciplinary teams are good



Thor BAA Overview



Thor BAA Overview

- 3 Phase program, 1 BAA
 - Phase 1 (18 Months)
 - Focus: Ability to detect known PAs
 - Prototype hardware developed
 - Phase 2 (18 Months)
 - Focus: Ability to detect unknown PAs
 - Possible Down select of PAD modalities that are underperforming
 - Phase 3 (12 Months)
 - Focus: Operationally relevant performance needed
 - Possible Down select of PAD modalities that are underperforming

Phase 1 (18 Months)

Phase 2 (18 Months)

Phase 3 (12 M)



Thor BAA Highlights

- A single BAA at the beginning
- Offeror teams will be required to make proposals severable for each modality
 - i.e. must have a plan for face, finger, and iris, but the government may choose to only fund a subset
 - May propose more than one approach to a single modality
 - E.g. you may propose developing a capacitive and optical fingerprint sensor
- The Government anticipates that proposals submitted under this BAA will be unclassified
- Multiple awards are expected
- Foreign participants and/or individuals may participate to the extent that such participants comply with any necessary Non-Disclosure Agreements, Security Regulations, Export Control Laws and other governing statutes applicable under the circumstances



Human Subjects Testing / Institutional Review Board (IRB)

- DNI / IARPA policy requires that a federal assurance (IRB) is provided for human subjects testing
- Note: Unlike some government agencies, we do not require an additional USG IRB approval
- You do not need to have an approved IRB prior to BAA submission, but you will need to comment on your plan/experience in this area in the BAA

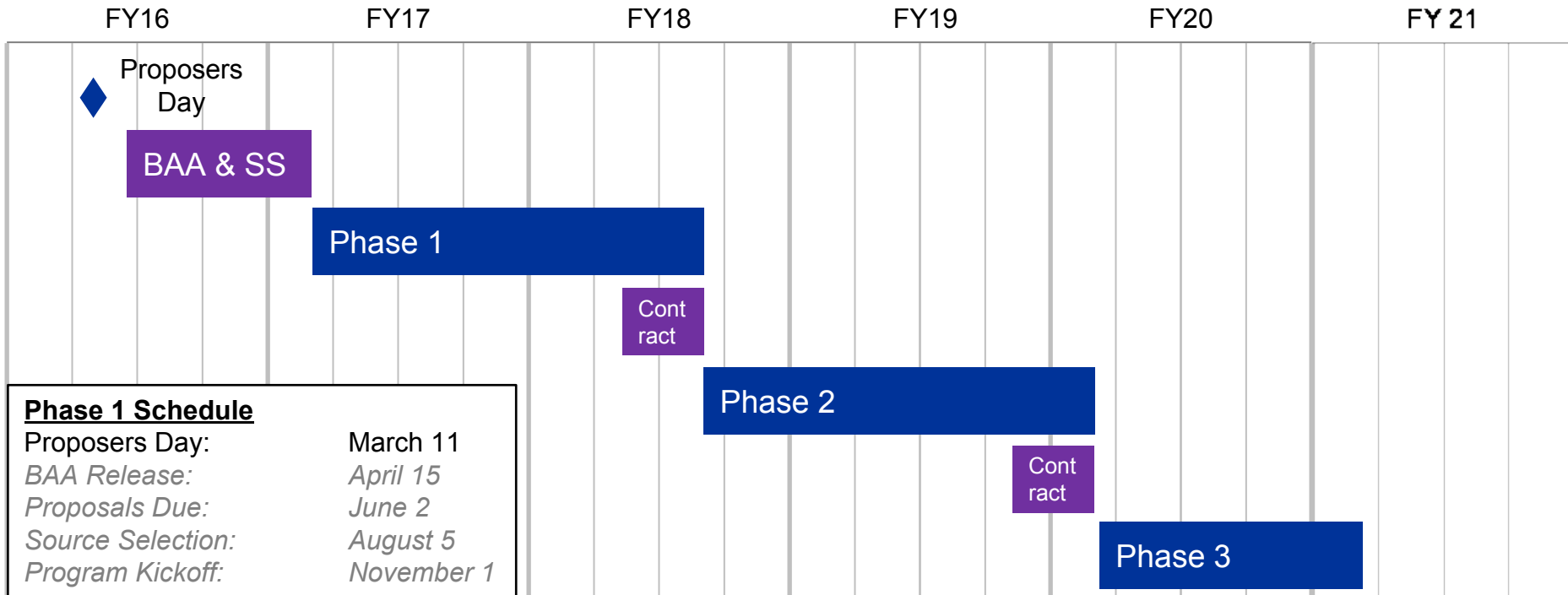


Items to be Addressed in a Thor Proposal

- Technical Approach
 - Sensors and algorithms used
 - Applicable use cases (e.g. high volume, high security, etc)
 - Anticipated PAD performance
- Constraints
 - Projected component cost, time to capture a sample
 - Legacy biometric recognition compatibility
- Management Plan
 - IRB



Notional/Target Schedule





Questions

- Please write on index card. Ok, to ask clarification verbally but speak loudly so all can hear.
- Discussions with the program manager are allowed until the BAA is released

Christopher.Boehnen@iarpa.gov



Odin Agenda Friday March 11th 2016

Time	Topic	Location / Attendees	Speaker
9:00am – 9:30am	Logistics, Program Introduction	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
9:30am – 10:10am	IARPA Overview	NOAA Open to Everyone	Dr. Stacey Dixon Deputy Director
10:10am – 10:20am	Break		
10:20am – 11:00am	Odin Technical Overview	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
11:00am – 11:30am	Odin BAA Overview	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
11:30am – 12:00pm	Doing Business with IARPA	NOAA Open to Everyone	IARPA Acquisitions
12:00pm – 12:30pm	Q&A Session	NOAA Open to Everyone	Dr. Chris Boehnen Program Manager
12:30pm – 1:00pm	Lunch – on your own		
1:00pm – 3:00pm	Poster Session and Teaming Discussions	NOAA No Government	Attendees
1:30pm – 2:00 pm	Check In MS2	MS2	Attendees
2:00 pm – 4:00 pm	Red Team	MS2 Minimum SECRET Clearance	Dr. Chris Boehnen Program Manager
4:00 pm – 5:00 pm	Red Team Teaming Discussions	MS2 No Government SECRET	Attendees

NOAA address is 5830 University Research Ct, College Park MD 20740

MS2 address is 5850 University Research Ct, Riverdale Park MD 20737