OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

CYBER-ATTACK AUTOMATED UNCONVENTIONAL SENSOR ENVIRONMENT (CAUSE)

PROPOSERS' DAY

January 21, 2015

Office for Anticipating Surprise

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)

CAUSE Program Proposers' Day Agenda

Time	Topic	Speaker
9:00am – 9:15am	**Welcome Remarks**	**Mr. Robert Rahmer** **Program Manager, IARPA**
9:15am – 9:45am	IARPA Overview and Remarks	Dr. Peter Highnam Director, IARPA
9:45am – 10:30am	CAUSE Program Overview	Mr. Robert Rahmer Program Manager, IARPA
10:30am – 10:45am	Break	Break
10:45am – 11:15am	Contracting Overview	Mr. Tarek Abboushi IARPA Acquisitions
11:15am – 11:45am	CAUSE Program Questions & Answers	Mr. Robert Rahmer Program Manager, IARPA
11:45am – 1:00pm	No Host Lunch	Lunch
1:00pm – 2:30pm	5-minute Capability Presentations	Attendees (**No Government**)
2:30pm – 4:00pm	Networking and Teaming Discussions	Attendees (**No Government**)

Proposers' Day Goals

- Familiarize participants with IARPA's interest in research to develop methods for detecting and forecasting cyber-attacks.
- Ask questions and provide feedback; this is your chance to alter the course of events.
- Foster discussion of synergistic capabilities among potential program participants, i.e., foster teaming. Take a chance: someone might have a missing piece of your puzzle

Disclaimer

- This presentation 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 requirements set forth in a Broad Agency Announcement (BAA).

Schedule

- Full Proposals are due ~45 days after BAA is published.
- Once BAA is released, questions can only be submitted and answered in writing via the BAA guidance.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

IARPA Overview

Dr. Peter Highnam

Office of the Director of National Intelligence

IARPA Mission and Method

IARPA's mission is to invest in high-risk/high-payoff research that has the potential to provide the U.S. with an overwhelming intelligence advantage over our future adversaries

- **Bring the best minds to bear on our problems**
  - Full and open competition to the greatest possible extent
  - World-class, rotational, Program Managers
- **Define and execute research programs that:**
  - Have goals that are clear, measureable, ambitious and credible
  - Employ independent and rigorous Test & Evaluation
  - Involve IC partners from inception to finish
  - Run from three to five years

Office of Incisive Analysis

"Maximizing Insight from the Information We Collect, in a Timely Fashion"

Large Data Volumes and Varieties	Social-Cultural and Linguistic Factors	Improving Analytic Processes
Providing powerful new sources of information from massive, noisy data that currently overwhelm analysts.	Analyzing language and speech to produce insights into groups and organizations.	Dramatic enhancements to the analytic process at the individual and group level.

Office of Smart Collection

"Dramatically Improve the Value of Collected Data"

Novel Access

Provide technologies for reaching hard targets in denied areas

Asset Validation and Identity Intelligence

Detect the trustworthiness of others

Advance biometrics in real-world conditions

Tracking and Locating

Accurately locate HF emitters and low-power, moving emitters with a factor of ten improvement in geolocation accuracy

Office of Safe and Secure Operations

"Counter Emerging Adversary Potential to Deny our Ability to Operate Effectively in a Globally-Interdependent and Networked Environment"

Computational Power	Trustworthy Components	Safe and Secure Systems
Revolutionary advances in science and engineering to solve problems intractable with today's computers	Getting the benefits of leading-edge hardware and software without compromising security	Safeguarding mission integrity in a hostile world

Office for Anticipating Surprise

"Detecting and Forecasting Significant Events"

S & T Intelligence	Indications & Warnings	Strategic Forecasting
Detecting and forecasting the emergence of new technical capabilities.	Early warning of social and economic crises, disease outbreaks, insider threats, and cyber attacks.	Probabilistic forecasts of major geopolitical trends and rare events.

How to engage with IARPA

- **Website: www.IARPA.gov**
  - Reach out to us, especially the IARPA PMs. Contact information on the website.
  - Schedule a visit if you are in the DC area or invite us to visit you.
- **Opportunities to Engage**:
  - **Research Programs**
    - Multi-year research funding opportunities on specific topics
    - Proposers' Days are a great opportunity to learn what is coming, and to influence the program
  - **"Seedlings"**
    - Allow you to contact us with your research ideas at any time
    - Funding is typically 9-12 months; IARPA funds to see whether a research program is warranted
    - IARPA periodically updates the topics of interest
  - **Requests for Information (RFIs) and Workshops**
    - Often lead to new research programs, opportunities for you to provide input while IARPA is planning new programs

Concluding Thoughts

- **Our problems are complex and truly multidisciplinary**
- **Technical excellence & technical truth**
  - Scientific Method
  - Peer/independent review
  - Full and open competition
- **We are always looking for outstanding PMs**
- **How to find out more about IARPA**:

  www.IARPA.gov
- **Contact Information**

  Phone: 301-851-7500

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

CYBER-ATTACK AUTOMATED UNCONVENTIONAL SENSOR ENVIRONMENT (CAUSE) Program Overview

Mr. Robert Rahmer, Program Manager

IARPA Office for Anticipating Surprise

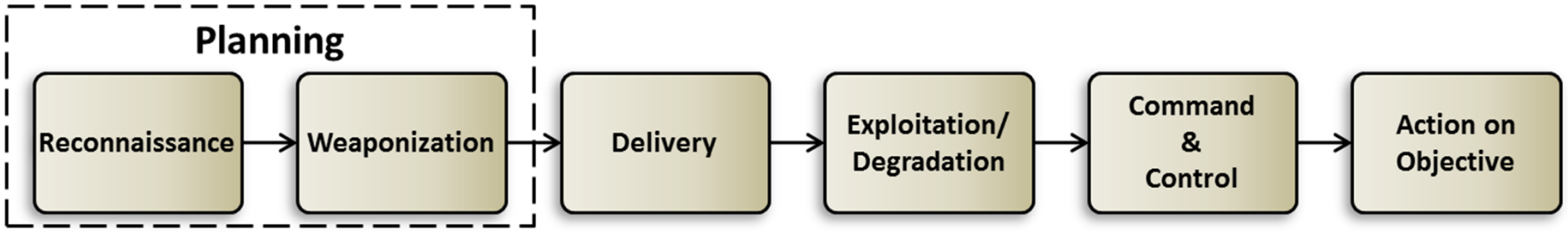
INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)

CAUSE Overview

- CAUSE is a multi-year research and development program.
- It seeks to develop new automated methods for forecasting and detecting cyber-attacks, hours to weeks earlier than existing methods.
- The CAUSE Program aims to develop and validate unconventional multi-disciplined sensor technology that will forecast cyber-attacks and complement existing advanced intrusion detection capabilities.

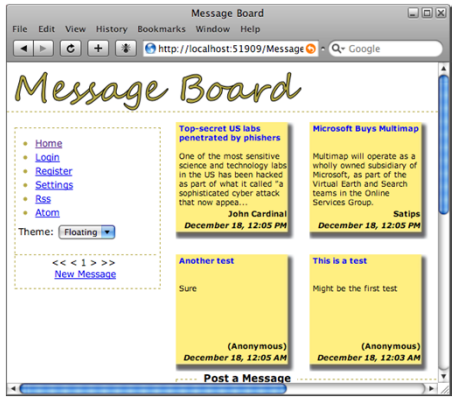
Background

- Cyber attacks evolve in a phased approach, which includes activities and observations before a significant event occurs: target reconnaissance, planning, and delivery.
- Detection of new cyber events and phenomena typically occurs in later phases of an attack
- Analysis occurs post-mortem to discover indicators from earlier phases.



Background

- Cyber Threat Intelligence capabilities often report threat actor activities, behaviors, and planning through observables from publicly available data, such as social media, news, chat, blogs, message boards, and many others, providing the means to infer motivations and intentions.



Background

- Published research states some of these publicly available data sources are useful in the early detection of other events such as disease outbreaks and macroeconomic trends.
  - News feeds, Twitter, blogs, and web search queries
- 2014 Verizon Data Breach Investigations Report
  - Victims of data breaches are notified by external parties **>75%** of the time.

Current Research

- Cyber attack prediction research has evolved, utilizing a combination of techniques:
  - Detailed knowledge of internal network infrastructures
  - Analysis of known vulnerabilities
  - Intrusion detection sensors for monitoring of an event in progress to predict future phases of an attack.

- Analysis of cyber actor behaviors and cultural dimensions has shown correlations between groups and cyber activities.

Current Research

- IARPA's Open Source Indicators (OSI) program developed methods for detecting / anticipating unexpected societal events (e.g., political crises, disease outbreaks) by fusing data of multiple types from multiple sources and utilizing ensemble machine learning methods.
- Few have researched methods for a probabilistic warning system for cyber defense that focuses on utilizing sensors external to an enterprise.

Key Technical Challenges

- Identify and evaluate **unconventional** and **technical** indicators in the earlier phases of cyber attacks that are **leading indicators** of later stages of the attack.
  - ***Looking for well-executed, non-traditional, creative ideas (e.g., black market sales analysis, cyber actor behavior models)***
- Create highly efficient algorithms that will process massive data streams from diverse data sets to extract signals from noisy data.
- Create techniques to fuse traditional technical indicator sensor data and alternate unconventional indicator data sources to develop automated probabilistic warnings.
- Identify and evaluate techniques that enable sharing of disparate threat contextual information and indicators among multiple organizations and security professionals to forecast an attack.

Evaluation

- Teams will deliver real-world cyber-attack warnings.
- The goal is to ***"Beat the Security Incident Reports."***
  - Teams choose sensors, data, and methods.
  - Teams are rewarded for early and accurate warnings of as many reportable events as possible.
- **Warning delivered to IARPA** =
  {Time stamp, Probability of attack, Cyber-attack details}
- **Event details** =
  (Event-Class, [Attacker], [Target], Event Time)
- Performers will send additional context about events which will be valuable to end users.
- Competitive forecasting tournament – the delivery of successive, better warnings is expected; each warning will be scored separately.

Industry Scope

- CAUSE is a research program, not an operational activity.
- In earlier phases, CAUSE will focus research on a particular U.S. business sector(s) that will be identified in the BAA. IARPA is choosing a business sector(s) with the following characteristics:
  - Organizations that have a variety of business areas
  - Sufficiently representative
    - Variety of attack types
    - Variety of existing external bad actors
  - Variety of publicly available data
  - Good ground truth data for training and testing
- Suggestions for data sharing partnerships with business sector(s) are welcome, please submit an index card.

Events and Scoring

- At kickoff, the Government team expects to provide a large list of significant cyber security events that occurred over the last 6 -18 months, for which an early warning would have been valuable.
- After kickoff, Government team expects to provide monthly "ground truth" – cyber security events for the last month, for which a warning would have been expected.
- Starting in Month 6, teams will deliver warnings to IARPA.
- Starting in Month 12, warnings delivered to IARPA are scored against Program milestones.

Events and Scoring

Scoring

- **Lead time:** Time warning delivered to IARPA compared to Time of earliest report of a security incident.
  Not necessarily time of event
- **Probability score:** Accuracy of probability assigned to security event.
- **Utility Time**: Time warning delivered to IARPA compared to the actual time of the security event.
- **Quality of Warning:** Match between event forecasted/detected and true event.
- **Recall and False Discovery Rate (FDR)**

- **Other assessments, qualitative and quantitative, will be performed by the Government team to evaluate each team's approach. Approaches will also be evaluated on the context within the warnings, as judged by potential users.**

Metrics

- **Lead Time (Drives earlier event detection)**
  - Time between warning and security incident report.
  - Teams will be asked to identify successive warnings for the same event. The Government team will use this information for assessment of team's approach for early detection.
- **Probability Score**
  - Quadratic score = $1 - (\boldsymbol{o}-\boldsymbol{p})^2$
  - ***p*** is the probability assigned to the warning, ***o*** is "ground truth": 1 if the event occurred, 0 if the event didn't occur within 7 days.
- **Utility (Drives forecasting)**
  - Time between warning and the actual event occurred as recorded in the security incident report. 3 day minimum is the goal. The Government team will use this information for assessment of team's approach to forecasting.

Metrics – Quality of Warning

- For each warning we calculate the quality $\mathbf{q = \alpha_1+\alpha_2+\alpha_3+\alpha_4}$
  - α_1 ~ Attack Classification;
  - α_2 ~ Attacker;
  - α_3 ~ Target;
  - α_4 ~ Event Time
  - This provides "partial credit" for partial warnings.

- Quality will use a typology of threat actors and targets to calculate the difference between ground truth for an attack; e.g., target:
  - Typology, α_3 = (Industry, Organization, Logical Address, Vulnerability)
  - Compare warning target with true target to get the vector (x_1, x_2, x_3, x_4), $x_i = 0$ if false, $x_i = 1$ if true
  - Location quality = $\frac{1}{4} x_1 + \frac{1}{4} x_1x_2 + \frac{1}{4} x_1x_2x_3 + \frac{1}{4} x_1x_2x_3x_4$

- For the time of the event, use *1- min(|predicted time – actual time|,7)/7*

Metrics & Scoring - Example

Warning

Warning	Time Stamp	Probability of Event	Attack Type	Source of Attack	Victim	Time of Attack
CW1:	8/1/2015	.25	Remote Exploit	Unknown	Business A	8/4/2015
CW2:	8/3/2015	.40	Remote Exploit	IP w.x.y.z	IP a.b.c.d	8/4/2015
CW3:	8/6/2015	.75	Remote Exploit	IP w.x.y.z	IP a.b.c.d, Vuln x-1	8/4/2015
Ground Truth:	8/10/2015	1	Remote Exploit	IP w.x.y.z	IP a.b.c.d, Vuln x-1	8/4/2015

Metrics & Scoring - Example

Quality Scores: (Victim)

Warning	Industry	Organization	Logical Address	Vulnerability	Score
CW1:	Industry X	Business A	-	-	.5
CW2:	Industry X	Business A	IP a.b.c.d	-	.75
CW3:	Industry X	Business A	IP a.b.c.d	Vuln x-1	1
Ground Truth:	Industry X	Business A	IP a.b.c.d	Vuln x-1	1

Overall Scores

Warning	Lead Time	Probability Score	Utility Time	Quality Score
CW1:	9 Days	.44	3 Days	2.5
CW2:	7 Days	.64	1 Day	3.08
CW3:	4 Days	.94	0 Days	3.67

Metrics

- **Recall:**

$$\frac{\text{Number of cyber events identified by Government team for which performer team sent a warning to IARPA with non-zero lead time and quality}}{\text{Total number of relevant cyber events identified by Government team}}$$

- **False Discovery Rate:**

$$\frac{\text{Number of false warnings identified by Government team for which performer team sent a warning to IARPA}}{\text{Total number of cyber event warnings sent to IARPA by performer team}}$$

Cyber-attack Events

Examples of events to forecast:

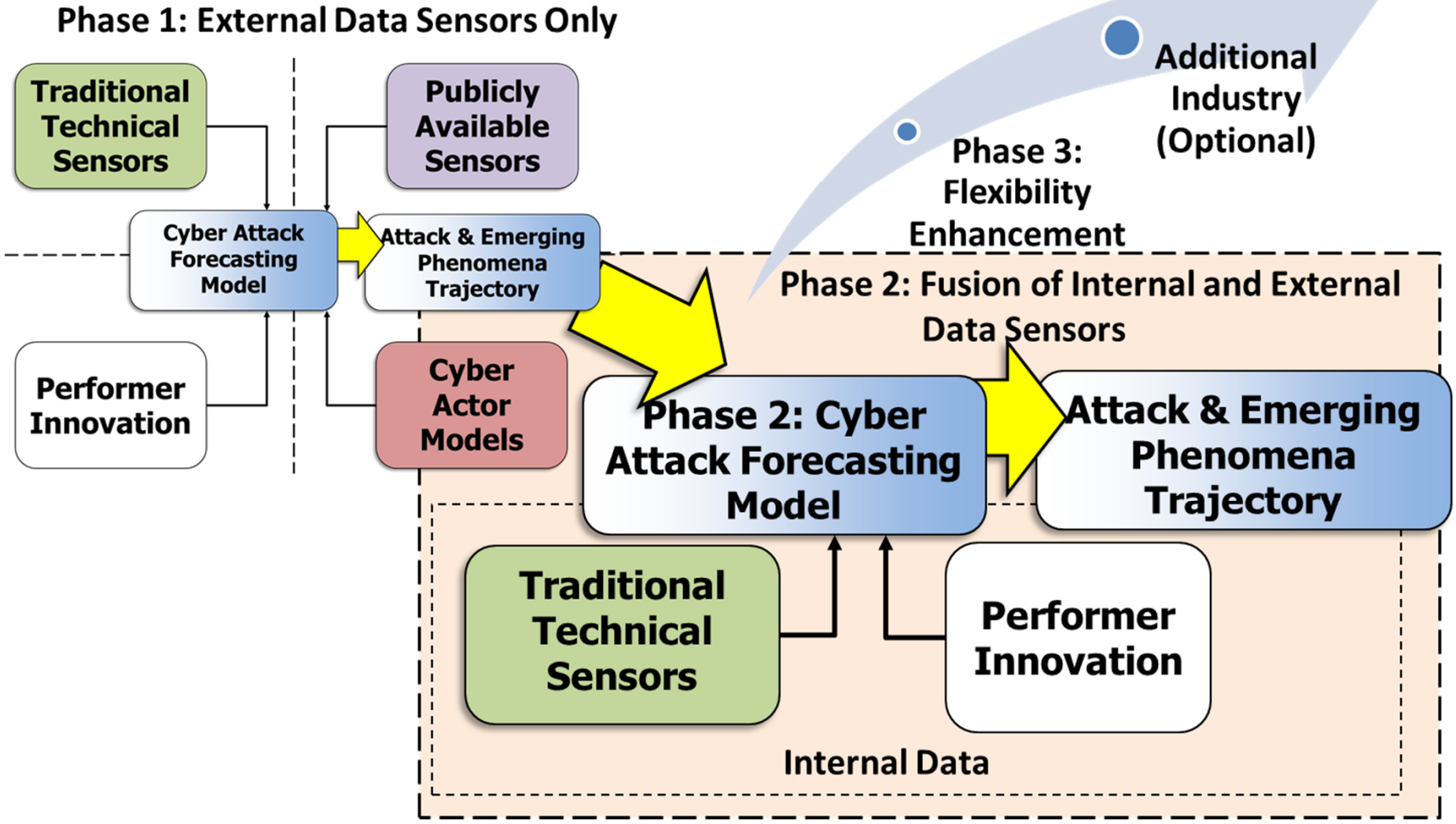
Cyber Event Type	Description
Unauthorized Access	An individual gains logical access without permission to a network, system, application, data, or other resource.
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources.
Malicious Code	Successful installation of malicious software that infects an operating system or application.
Scans/Probes/ Attempted Access	Activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.

If you have any suggestions, please submit an index card!

Warning Generation

- It is expected that the technology developed under this effort will have **no** "*human in the loop.*"
- Experents can help develop and train the system, but they ***will not*** manually generate warnings, guide the system, or filter warnings before they are sent to IARPA.
- Teams' systems must include an audit trail for each warning, listing relevant evidence and weights.
- Warnings that are related should be explicitly identified for additional evaluation by the Government team.
  - Successive warnings for the same event,
  - Warning for mutually exclusive events.

Program Structure



Program Structure

Phase 1 (18 months): External Data Sources	
Goal 1	Identify predictive threat signals from technical and unconventional sources
Goal 2	Perform data classification and training for model development
Goal 3	Generate Warnings
Phase 2 (12 months): Data Fusion w/Internal Data Sources	
Goal 1	Create a data fusion model for integrating external and internal data
Goal 2	Research highly effective algorithms for processing massive data
Goal 3	Generate Warnings
Phase 3 (12 months): Solution Flexibility Enhancement	
Goal 1	Evaluate solutions' flexibility to integrate within a new organization
Goal 2	Evaluate capability for forecasting cyber attacks across multiple organizations
Goal 3	Generate Warnings

Milestones

Metric	Phase 1	Phase 2	Phase 3
Mean Lead Time	2 days	3 days	5 days
Mean Probability Score	2.4	3	3.2
Mean Utility Time	1 day	2 days	3 days
Mean Quality Score	2	3	3.5
Recall	0.5	0.7	0.8
False Discovery Rate (FDR)	< 0.5	< 0.2	< 0.1

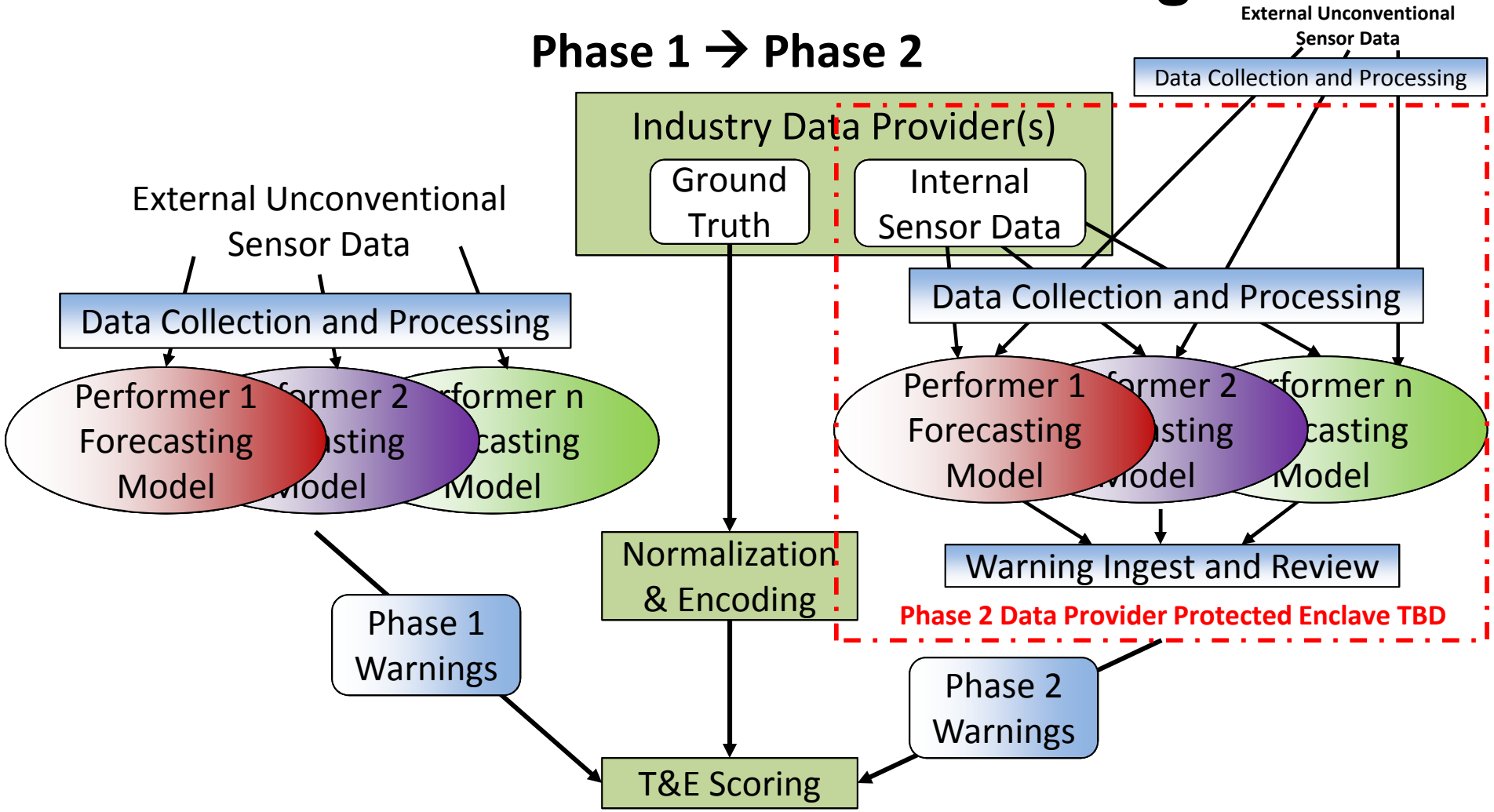
What CAUSE is not

- **Not a program focused on:**
  - Identification of specific individuals
  - Collection mechanisms that require directed participation by individuals
- **Not narrowly focused on a single data source or type**
- **Not a program on developing intrusion detection capabilities leveraging internal data**
- **Not a program focused on insider threats**
- **Not a program on data visualization**

Data

- Acquisition/collection of external data will require resources (time and budget) by each team, and data requirements will likely overlap across teams.
- In later phases, performers will use internal data from participating U.S. business sector organization(s).
  - Performers may want to access their own or another organization's internal technical data sources earlier in the program to aid R&D of novel sensors to support future program goals.
  - BAA will ask bidders to identify internal data sources required to extract novel signals from participating U.S. business sector organization(s).

CAUSE Notional Data Flow Diagram



Team Composition

- Given the combination of technical challenges, we anticipate teams will possess expertise in:
  - Computer science
  - Data science
  - Social and Behavioral science
  - Mathematics and statistics
  - Content extraction
  - Information theory
  - Cyber-security
  - Software development

Teaming

- **Because of the many challenges presented by this program, both depth and diversity will be beneficial.**
  - **Throughput**. Consider all that you will need to do, all the ideas you will need to test.
    - Make sure you have enough people with the right expertise to do the job.
    - Sufficient resources to follow critical path while still exploring alternatives – risk mitigation
  - **Completeness**. Teams should not lack any capability necessary for success, e.g., mitigate any dependency risks
  - **Tightly knit teams.**
    - *Clear, strong, management, and single point of contact*
    - No loose confederations
    - Each team member should be contributing significantly to the program goals. Explain why each member is important, i.e., if you didn't have them, what wouldn't get done?

Remember, you may be very accomplished, but can you do it all?

Summary

- CAUSE seeks to develop new automated methods for forecasting and detecting cyber-attacks, hours to weeks earlier than existing methods.
- The Program aims to develop and validate unconventional multi-disciplined sensor technology that will forecast cyber-attacks and complement existing advanced intrusion detection capabilities.
- We are looking for well-executed, creative ideas for unconventional sensors.
- The BAA supersedes anything presented or said at the Proposers' Day by IARPA.

Questions?

If you have questions, suggestions, and comments – please submit an index card now!

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Contracting Overview

Mr. Tarek Abboushi

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)

Doing Business with IARPA - Recurring Questions

- Questions and Answers (http://www.iarpa.gov/index.php/faqs)
- Eligibility Info
- Intellectual Property
- Pre-Publication Review
- Preparing the Proposal (Broad Agency Announcement (BAA) Section 4)
  - Electronic Proposal Delivery (https://iarpa-ideas.gov)
- Organizational Conflicts of Interest (http://www.iarpa.gov/index.php/working-with-iarpa/iarpas-approach-to-oci)
- Streamlining the Award Process
  - Accounting system
  - Key Personnel
- IARPA Funds Applied Research
- RECOMMENDATION: Please read the entire BAA

Responding to Q&As

- Please read entire BAA before submitting questions
- Pay attention to Section 4 (Application & Submission Info)
- Read Frequently Asked Questions on the IARPA @

  http://www.iarpa.gov/index.php/faqs

- Send your questions as soon as possible
  - CAUSE BAA: dni-iarpa-baa-15-06@iarpa.gov
  - Write questions as clearly as possible
  - Do NOT include proprietary information

Eligible Applicants

- Collaborative efforts/teaming strongly encouraged
  - Content, communications, networking, and team formation are the responsibility of Proposers
- Foreign organizations and/or individuals may participate
  - Must comply with Non-Disclosure Agreements, Security Regulations, Export Control Laws, etc., as appropriate, as identified in the BAA

Ineligible Organizations

Other Government Agencies, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), and any organizations that have a special relationship with the Government, including access to privileged and/or proprietary information, or access to Government equipment or real property, are not eligible to submit proposals under this BAA or participate as team members under proposals submitted by eligible entities.

Intellectual Property (IP)

- Unless otherwise requested, Government rights for data first produced under IARPA contracts will be UNLIMITED.
- At a minimum, IARPA requires Government Purpose Rights (GPR) for data developed with mixed funding
- Exceptions to GPR
  - State in the proposal any restrictions on deliverables relating to existing materials (data, software, tools, etc.)
- If selected for negotiations, you must provide the terms relating to any restricted data or software, to the Contracting Officer

Pre-Publication Review

- Funded Applied Research efforts, IARPA encourages:
  - Publication for Peer Review of **UNCLASSIFIED** research

- Prior to public release of any work submitted for publication, the Performer will:
  - Provide copies to the IARPA PM and Contracting Officer Representative (COR/COTR)
  - Ensure shared understanding of applied research implications between IARPA and Performers
  - Obtain IARPA PM approval for release

Preparing the Proposal

- Note restrictions in BAA Section 4 on proposal submissions
  - Interested Offerors must register electronically IAW instructions on: **https://iarpa-ideas.gov**
  - Interested Offerors are strongly encouraged to register in IDEAS at least 1 week prior to proposal "Due Date"
  - Offerors must ensure the version submitted to IDEAS is the "Final Version"
  - Classified proposals – Contact IARPA Chief of Security
- BAA format is established to answer most questions
- Check FBO for amendments & IARPA website for Q&As
- BAA Section 5 – Read Evaluation Criteria carefully
  - e.g. "The technical approach is credible, and includes a clear assessment of primary risks and a means to address them"

Preparing the Proposal (BAA Sect 4)

- Read IARPA's Organizational Conflict of Interest (OCI) policy: **http://www.iarpa.gov/index.php/working-with-iarpa/iarpas-approach-to-oci**
- See also eligibility restrictions on use of Federally Funded Research and Development Centers, University Affiliated Research Centers, and other similar organizations that have a special relationship with the Government
  - Focus on possible OCIs of your institution as well as the personnel on your team
  - See Section 4: It specifies the non-Government (e.g., SETA, FFRDC, UARC, etc.) support we will be using. If you have a potential or *perceived* conflict, request waiver as soon as possible

Organizational Conflict of Interest (OCI)

- If a prospective offeror, or any of its proposed subcontractor teammates, believes that a potential conflict of interest exists or may exist (whether organizational or otherwise), the offeror should promptly raise the issue with IARPA and submit a waiver request by e-mail to the mailbox address for this BAA at **dni-iarpa-baa-15-06@iarpa.gov**.
- A potential conflict of interest includes but is not limited to any instance where an offeror, or any of its proposed subcontractor teammates, is providing either scientific, engineering and technical assistance (SETA) or technical consultation to IARPA. In all cases, the offeror shall identify the contract under which the SETA or consultant support is being provided.
- Without a waiver from the IARPA Director, neither an offeror, nor its proposed subcontractor teammates, can simultaneously provide SETA support or technical consultation to IARPA and compete or perform as a Performer under this solicitation.

Streamlining the Award Process

- Cost Proposal – we only need what we ask for in BAA
- Approved accounting system needed for Cost Reimbursable contracts
  - Must be able to accumulate costs on job-order basis
  - DCAA (or cognizant auditor) must approve system
  - See **http://www.dcaa.mil** , "Audit Process Overview - Information for Contractors" under the "Guidance" tab
- Statements of Work (format) may need to be revised
- Key Personnel
  - Expectations of time, note the Evaluation Criteria requiring relevant experience and expertise
- Following selection, Contracting Officer may request your review of subcontractor proposals

IARPA Funding

- IARPA funds Applied Research for the Intelligence Community (IC)
  - IARPA cannot waive the requirements of Export Administrative Regulation (EAR) or International Traffic in Arms Regulation (ITAR)
  - Not subject to DoD funding restrictions for R&D related to overhead rates

- IARPA is not a DOD organization

Disclaimer

- This is Applied Research for the Intelligence Community
- Content of the Final BAA will be specific to this program
  - The Final BAA is being developed
  - Following issuance, look for Amendments and Q&As
  - There will likely be changes
- The information conveyed in this brief and discussion is for planning purposes and is subject to change prior to the release of the Final BAA.

QUESTIONS ?

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

CAUSE Program Q&A

Mr. Robert Rahmer, Program Manager

IARPA Office for Anticipating Surprise

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu