OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Scientific advances to Continuous Insider Threat Evaluation (SCITE)

Dr. Paul Lehner
April 16, 2015

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)

SCITE Program Proposers' Day Agenda

Time	Topic	Speaker
8:00am –	Registration Opens	
9:00am – 9:15am	Welcome Remarks	Dr. Paul Lehner Program Manager, IARPA
9:15am – 9:30am	IARPA Overview and Remarks	Dr. Peter Highnam Director, IARPA
9:30am – 10:15am	SCITE Program Overview	Dr. Paul Lehner Program Manager, IARPA
10:15am – 10:45am	Break	Break
10:45am – 11:15am	Doing Business with IARPA	Mr. Tarek Abboushi IARPA Acquisitions
11:15am – 11:45am	SCITE Program Questions & Answers	Dr. Paul Lehner 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 the SCITE Program.
- 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	Asset Validation and Identity Intelligence	Tracking and Locating
Provide technologies for reaching hard targets in denied areas	Detect the trustworthiness of others Advance biometrics in real-world conditions	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

Detecting and forecasting the emergence of new technical capabilities.

Indications & Warnings

Early warning of social and economic crises, disease outbreaks, insider threats, and cyber attacks.

Strategic Forecasting

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

SCITE
Program Overview

LEADING INTELLIGENCE INTEGRATION

Dr. Paul Lehner
April 16, 2015

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)

SCITE Overview

- SCITE is a multi-year research and development program.

- The SCITE Program seeks to advance the science and practice of insider threat detection through two separate research tracks
  - Research into modeling and forecasting the performance of existing and proposed insider threat detection enterprises
  - Research to develop a new class of indicators, called active indicators, and associated automated detection tools

Background and Definitions

- Insider threats: Individuals with privileged access within an organization who are, or intend to be, engaged in malicious behaviors such as espionage, sabotage or violence.

- Potential threat: Analyst-specified set of behavioral criteria that may be indicative of a current or future insider threat; for example:
  - Currently engaged in exfiltration of sensitive data
  - Disgruntled and angry about their work situation

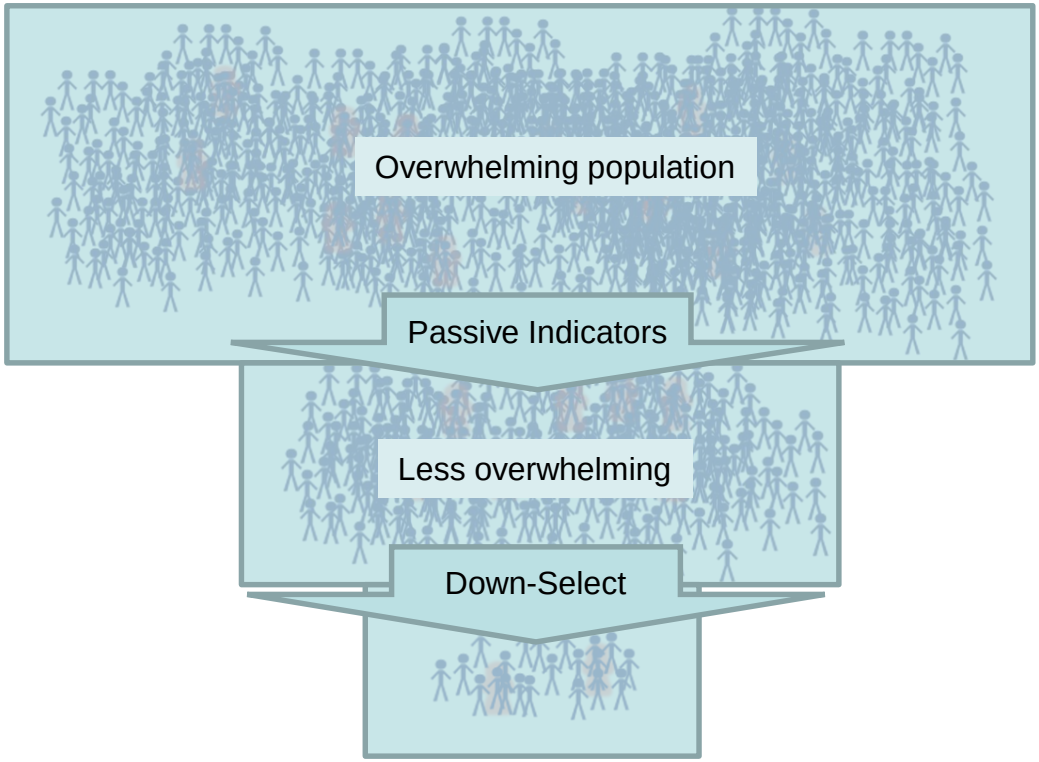
- Down-select algorithm: Any collection of algorithms that automatically sort through alerted indicators to select a subset of users for analysts to examine
  - Can range in complexity from simple analyst-specified decision rules to engineered Bayesian fusion/decision models to machine-learned pattern detectors

- Inference enterprise: A collection of people, tools, data sources, algorithms, and processes devoted to making inferences
  - SCITE focus is on the automated portion of inference enterprises devoted to finding potential threats

State of Current Practice

- Insider Threat Detection Programs
  - Usually associated with information infrastructure protection
  - Involves automated monitoring of behavior on internal information infrastructure
    - Searches, downloads, purging, printing, mobile storage, email content, etc.
    - Automated tools to detect possible instances of indicators
    - Automated aggregation and down-select algorithms
- Continuous Evaluation
  - Derived from Personnel Security authority to grant clearances and access
  - Involves automated monitoring of external data sources
    - Financial, legal, criminal, real estate, travel, etc.
    - Automated Continuous Evaluation System (ACES) or other tools to download records
    - Beginning to implement automated detectors and down-select algorithms
- Both
  - Rely on passive monitoring for indicative behaviors – passive indicators
  - Experience overwhelming numbers of false alarms
  - Limited ability to effectively down-select to manageable subpopulation for analysis

Summary of Current Practice



A few potential threats in a large diverse population

Weak association between indicators and potential threats

Large diverse subpopulation

Forced to reduce to

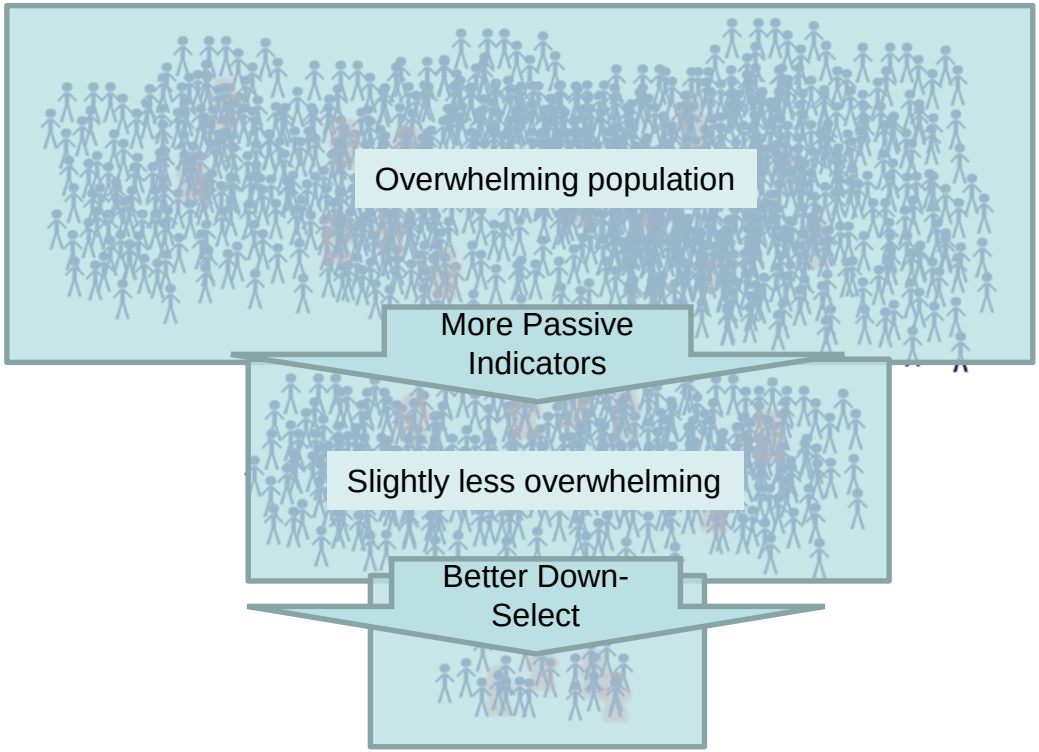
Small group that contains a few potential threats

Opaque understanding of inference enterprise performance

State of Current Research

- Forensic analysis of historical cases
  - No strong relationships/indicators, but various probabilistic relationships/correlates
- Threat modeling
  - Formal representation of probabilistic relationships
  - Bayesian network is representation of choice
- Some experimentation on new indicators
  - Download behavior patterns of normal vs. (red team) espionage users
- Diversity of new detectors for hypothesized indicators
  - Anomaly detection relative to individual baseline, work group, standard work processes, …
  - Negative sentiment detection in text sources such as emails, message boards, etc.
  - Various ensemble and fusion approaches
  - Limited evaluation of accuracy, false alarm rates, etc.
- Continue to rely on passive indicators

Summary of Current Research



A few potential threats in a large diverse population

More weak associations

Larger subpopulation

Hopefully much better

Small group that hopefully contains a few more potential threats

Still opaque understanding of inference enterprise performance

Practice and Research: Enterprise Modeling

- Enterprise Engineering "… is an integrated set of disciplines for building an enterprise, its processes, and systems." James Martin (1995) *The Great Transition: Using the seven disciplines of enterprise engineering to align people, technology.* AMACOM Books, NY
- Enterprise model "… Enterprise modeling [is used] either as a technique to represent and understand the structure and behavior of the enterprise, or as a technique to analyze business processes, and in many cases as support technique for business process reengineering." Mertins, K., & Jochem, R. (2005). Architectures, methods and tools for enterprise engineering. *International Journal of Production Economics*, *98*(2), 179-188.
- Enterprise models are intended to support enterprise (re)engineering.
  - Function models (often IDEF charts)
  - Data models
  - Business process models (often workflow models)
  - System architectures
- Current practice and research on enterprise engineering and modeling do not address inference or decision accuracy

SCITE Program Tracks

- Track 1: Research to design and test *Inference Enterprise Models* to detect various types of potential threats

- Track 2: Research to design and test *active indicators* that evoke indicative responses from insiders engaged in espionage activities

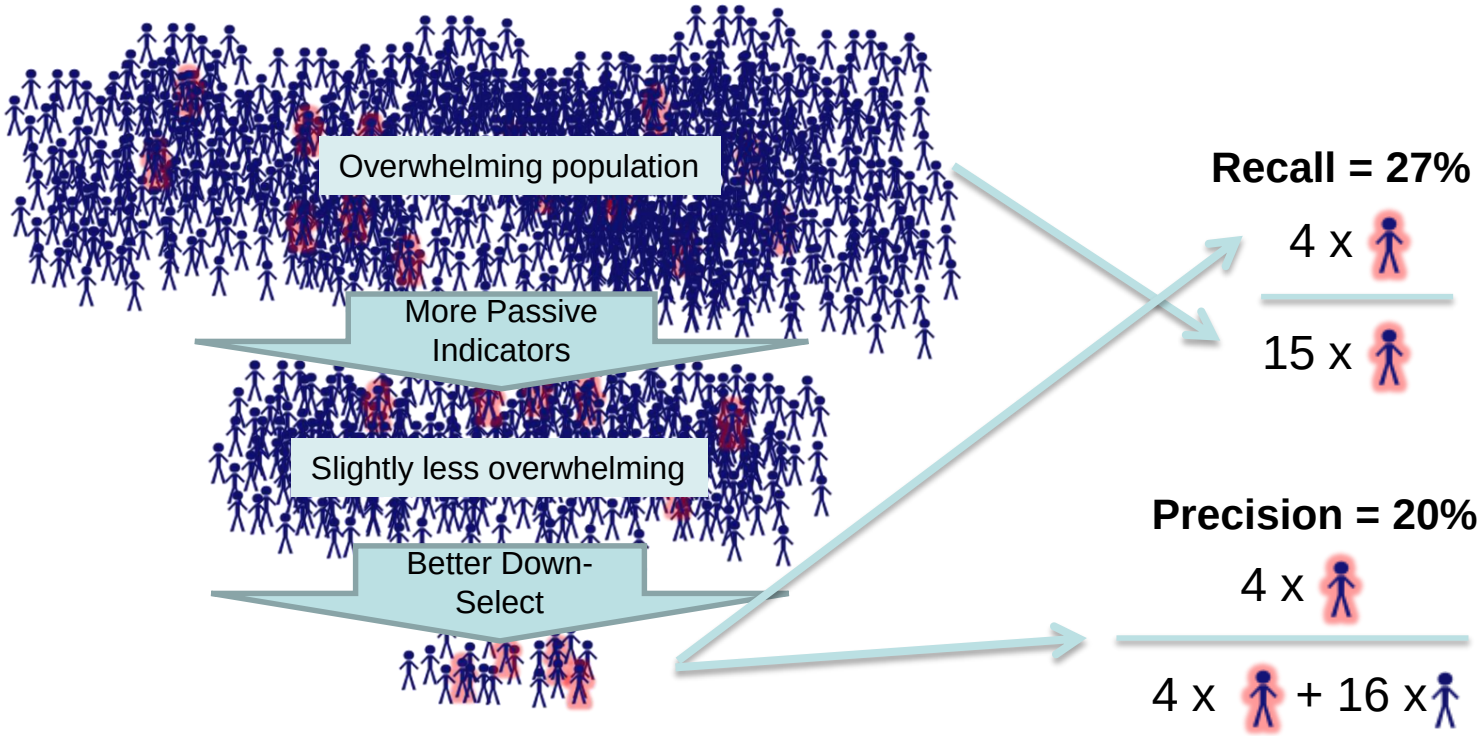
- What SCITE is <u>not</u> researching
  - New passive indicators
  - New down-select algorithms
  - New profiles or psychological theories of insider threats
  - However, IEM research may involve modeling of enterprises that seek to find insiders that match a new psychological profile using new passive indicators and down-select algorithms

Track 1: Inference Enterprise Modeling

- Research in *Inference Enterprise Engineering* to develop models that
  - Estimate performance of existing inference enterprises
  - Forecast performance impact of proposed changes to an inference enterprise
  - General focus on enterprises that find *low-probability events with low-accuracy sensors*
  - Targeted focus on modeling automated systems to detect potential threats

- Research challenges
  - Represent causal probabilistic relationships between behaviors, indicators, detectors and down-select algorithms
  - Processes to elicit and construct causal maps of probabilistic relationships
  - Integrate diverse approaches to estimating parameter values
  - Tradeoff model fidelity (e.g. modeling complex interactions) and parameter fidelity (e.g. avoid modeling interactions to improve parameter assessment accuracy)
  - Derive performance estimates and associated certainty intervals

Track 1 Objective: Transparent Understanding of Existing and Proposed Automated Monitoring Processes



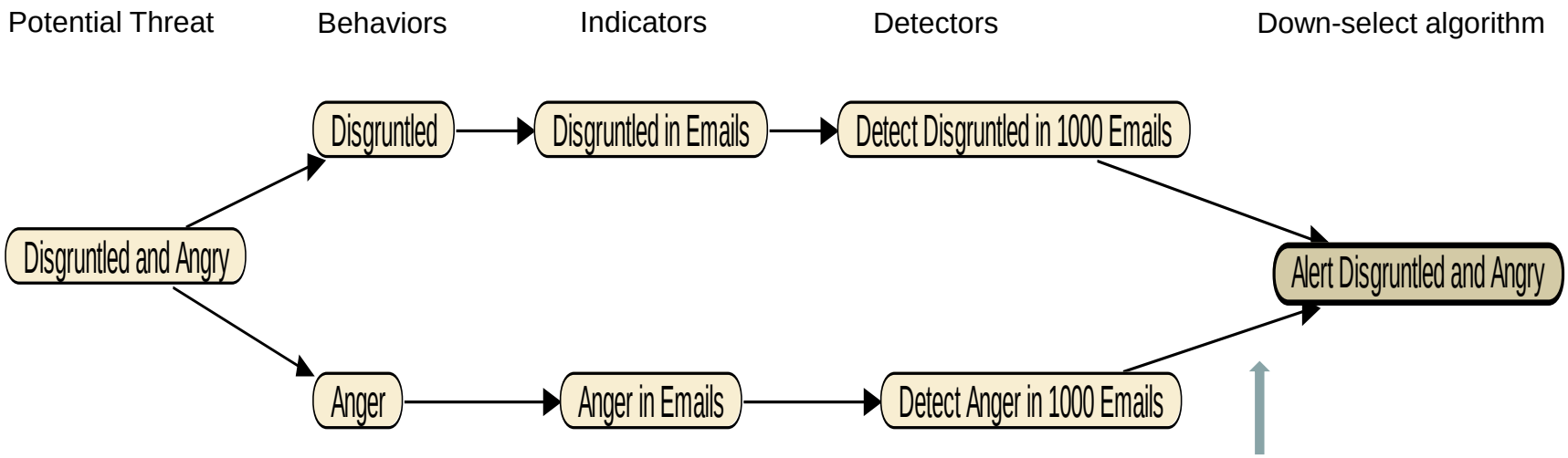
Example of Inference Enterprise Modeling

(Not a technical suggestion)

- An agency is exploring whether to use a sentiment analysis tool
  - Compared tool assessments to independent manual coding of each of ~20,000 randomly selected emails
- Two empirical results from one tool
  - Detecting Disgruntlement: Recall 17%, Precision 22%, Alert rate 2.9%
  - Detecting Anger: Recall 22%, Precision 6%, Alert rate 0.8%
- Imagine an organization with 1,000 employees sending 30 emails per day
  - 30,000 emails; 240 alerts for anger; 870 alerts for disgruntlement
  - Over 1,110 alerts per day for just two emotions of concern. More alerts than employees!
- How might this (apparently poor-performing) tool be used effectively?

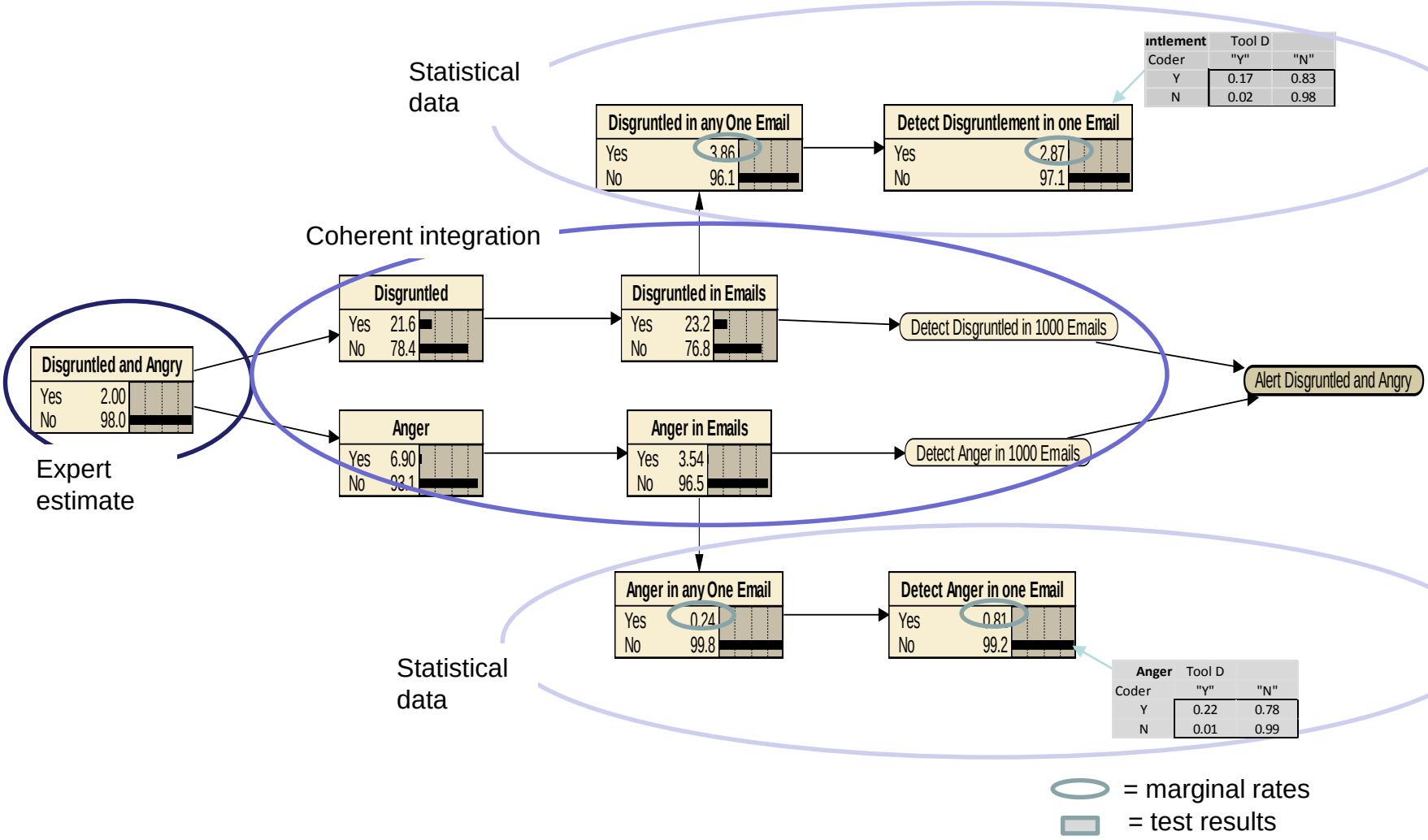
Note: US estimate in 2013 was 37 emails per day from corporate employees

Causal Chain from Potential Threat to Down-Select Decisions

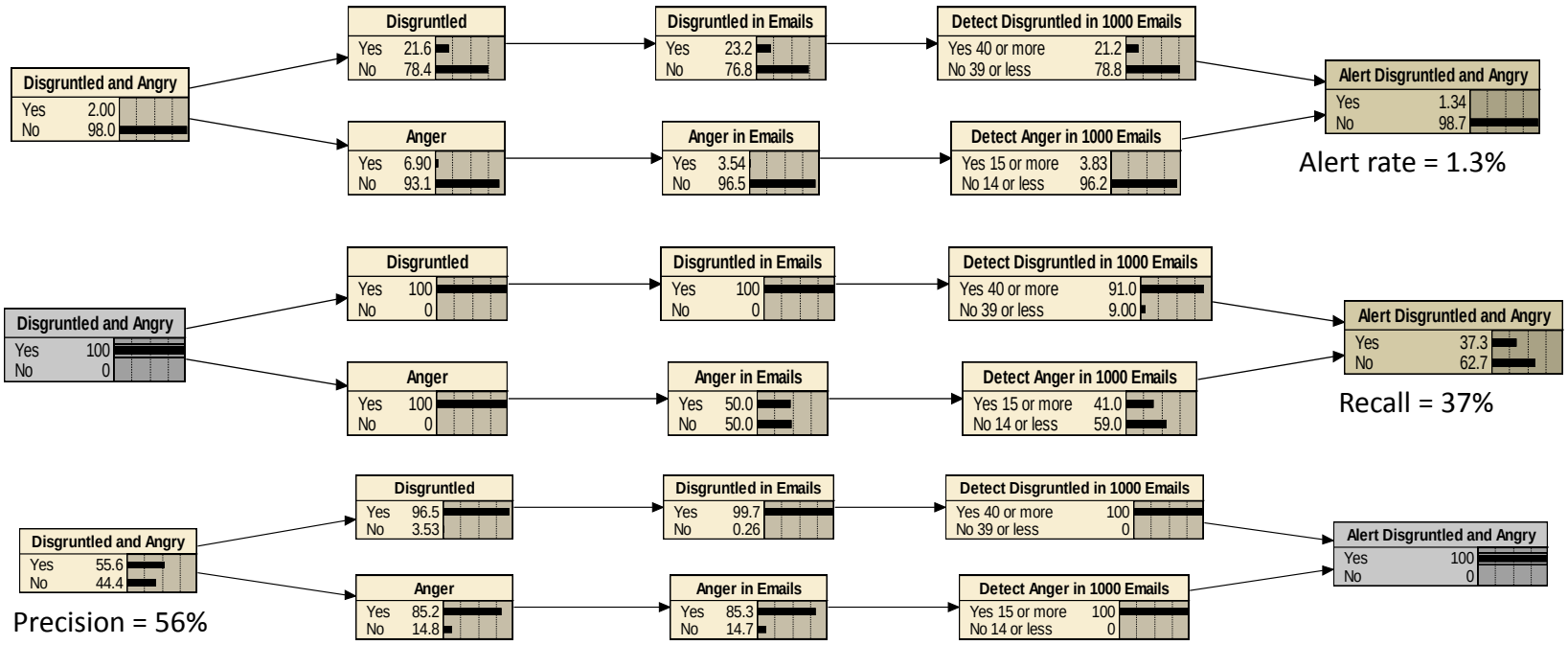


Select if both disgruntled and angry (D&A) are detected in last 1,000 emails.

Integrating Statistical Data and Subjective Estimates



Deriving Performance Estimates



	Tool Performance	Enterprise Performance
Alert Frequency	1,110	13
Recall	~20%	37%
Precision	~12%	56%

IEM Research

- Government team will provide performers with a series of increasingly challenging *redacted challenge problems* where for each problem
  - Government team will provide an initial summary expert judgment/statistical description of a portion of a third-party operational insider threat system
    - Perhaps with proposed enhancements (new tools, indicators, algorithms, …)
    - Government team will respond as feasible to requests for additional information
  - Performers will develop their inference enterprise models and submit forecasts of the performance of the automated system as point estimates plus certainty intervals (e.g. Recall = 0.4), with 60% certainty that Recall $\in$ [0.3, 0.5].

- Accuracy of performer forecasts will be estimated as follows:
  - Forecasts will be assessed by analyst review of users selected by stratified sampling on the inference
  - Espionage behaviors (special case):
    - There will be (red team) users who are paid espionage players on the third-party system
    - Analysts performing the reviews will know who these players are

Stratified Sampling on the Inference

- Imagine that
  - Out of 10,400 (third-party) employees, system alerted "Disgruntled and Angry" (D&A) on 400
  - Randomly select for analysis
    - 100 that alert for D&A (25% of 400)
    - 100 that do not alert for D&A (1% of 10,000)
  - Obtain following results for this stratified sample

Test Results	Alert D&A	Not alert D&A
Analysts confirm D&A	50	5
Analysts deny D&A	50	95

Government team analysts review a sufficiently sized sampling of alert and non-alert cases.

- What are the performance estimates for the entire population of 10,400 employees?

Stratified Sampling on the Inference

Test Results	Alert D&A	Not alert D&A
Analysts confirm D&A	50	5
Analysts deny D&A	50	95
Sampling rate	25%	1%

Population Estimates	Alert D&A	Not alert D&A
Analysts would confirm D&A	200	500
Analysts would deny D&A	200	9,500

Estimate number of potential threats, here being number of insiders who are D&A

Estimate = 700

95% CI ~ (250,1100)

	Independent Estimate		IEM Forecast
Recall	= 28.6%	(200/700)	37.0%
Precision	= 50.0%	(200/400)	56.0%
Alert Rate	= 3.8%	(400/10,400)	1.3%

This independent estimation process does not require *a priori* construction of (artificial) test sets or knowledge of the potential threats

IEM Research Phases, Metrics and Milestones

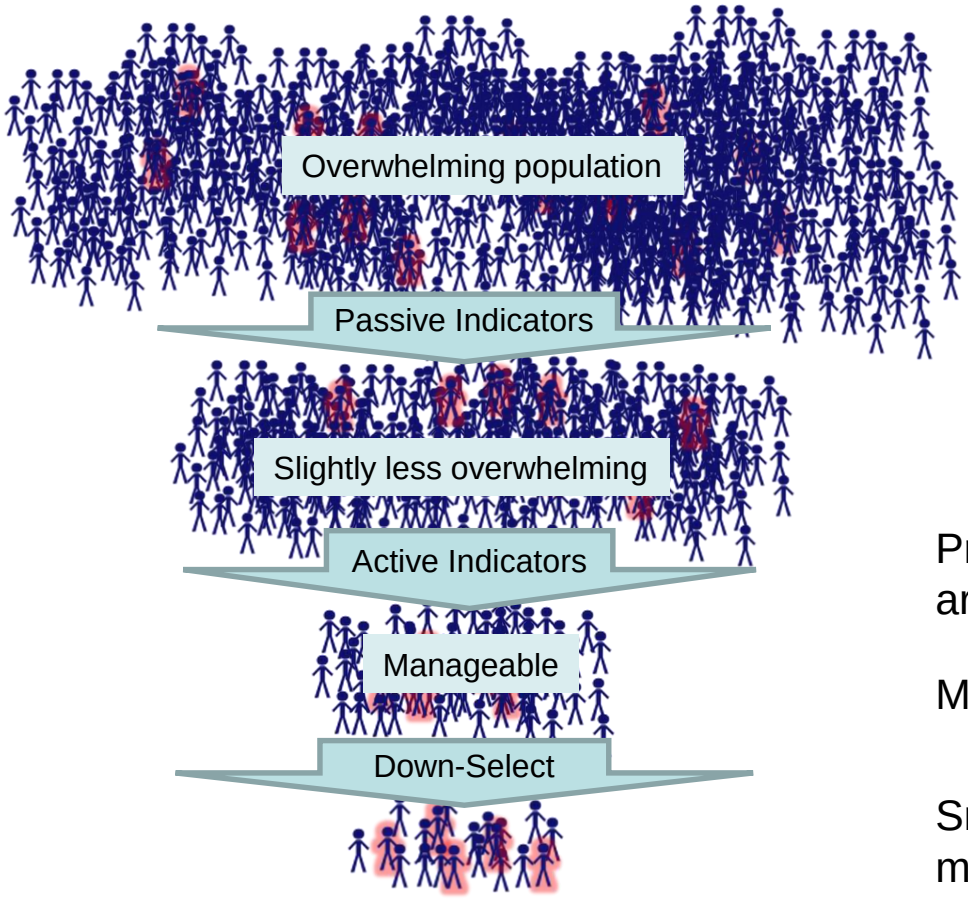
	Phase 1		Phase 2		Phase 3	
	6	12	18	24	30	36
Number of potential threat types & detectors	2/10	4/20	10/50	20/100	20/200	40/400
Challenge elements	Existing detectors, indicators & algorithms		+ New indicators, detectors & algorithms		+ IEM-derived down-select rules	
Certainty interval calibration metric: Percent of ground truth within forecast 60% certainty intervals	n/a	60 ± 20%	60 ± 15%	60 ± 15%	60 ± 10%	60 ± 10%
Certainty interval precision metric: Average range of 60% certainty interval	n/a	±25%	±20%	±20%	±15%	±15%

Track 2: Active Indicators and Evoke-alert Tools

- Research in finding *active indicators* that evoke indicative responses from insiders engaged in espionage
  - *Evoke-alert tools* that automatically, selectively initiate stimuli and test for indicative responses
  - Indicator and tool development specifically focused on detecting espionage behavior

- Research challenges
  - Discovery of *robust, noninvasive* and *discreet*-stimulus *indicative*-response behaviors that distinguish malicious from benign users
  - Progress toward a theory of active indicators supporting generalizations beyond just the specific indicators tested
  - Development of accurate detectors that detect instances when indicative responses occur

Track 2 Objective: Massively Reduce False Alarm Rates



Proactive stimulus-response tests that are adjuncts to passive indicators

Massively reduce subpopulation

Small group that includes many more potential threats

Illustrative Examples of Possible Active Indicators
(Not technical suggestions)

- **Exfiltrating or deleting files before possible inspection**
  - Passive Indicator: Downloads files outside of work scope
  - Evoke-stimulus: Notification that their system's hard drive will be inspected due to general backup problems, possible corruption, etc.
  - Indicative Responses: Large quantities of files are deleted, moved, or downloaded to mobile storage
  - Normal User Response: Nothing, the benign user knows that the files they need are backed up or the profile is roaming and nothing important is saved on the hard drive
  - Detectors/Alert: Downloads files to removable storage within 24 hours after message; deletes large numbers of files within 24 hours after message

- **Avoids making explicit request to access selected sites**
  - Passive Indicator: Repeatedly accessing internal sites outside of work scope
  - Evoke-stimulus: Block access to site until request and justification are provided to system
  - Indicative Responses: Failure to request access yet continued attempts to access site
  - Normal User Response: Request access to site with justification provided or never return to site because they do not need information enough to request access
  - Detectors/Alert: Detect continued attempts to access without justification

Illustrative Examples of Possible Active Indicators
(Not technical suggestions)

- **Failure to correct foreign contact or travel record**
  - Passive Indicator: Discovery of unreported foreign contact or travel
  - Evoke-Stimulus: Issue reminder or "new training" on reporting requirements implying "no cost" opportunity to correct record
  - Indicative Responses: Failure to correct record
  - Normal User Response: Correct record or ask clarifying questions in attempt to understand requirements (bringing attention to self for any reason)
  - Detector/Alert: Change in record or record of clarification query

Active Indicators Research

- Performers will develop and test active indicators and associated detectors
  - Propose and test at least two new active indicators every six months
  - Test each potential indicator in at least two settings (to support robustness claim)
    - May be different test environments, settings within a single test environment, different levels of knowledge about active indicators, etc.
  - Progress toward theory supporting generalizations beyond the specific indicators tested
  - Develop software that detects instances when an indicative response has occurred

- Performers provide own test environment for testing indicators and detectors
  - Users engaged in espionage behavior and normal users, both receive active stimuli and are monitored for their response; Possible examples (not technical suggestions):
  - Example 1: Users on an existing information infrastructure engage in an “espionage game” where they are tasked to find, access and exfiltrate data from selected sites without being detected
  - Example 2: An environment where some users will naturally engage in espionage behaviors (e.g., stealing cheat codes in a game environment)

Active Indicators Research

- Performer experiments should include dependent variables that support assessment of individual indicators against the following criteria:
  - Discreet: users are unaware that the stimulus is related to insider threat detection
  - Indicative: users engaged in espionage activities often respond differently than normal users
  - Robust: the indicative response must occur across different settings
  - Noninvasive: reacting to the stimulus does not negatively impact normal workflows

- Government team will perform additional testing
  - Government team will have its own test environment(s)
  - Performers will not be privy to any results of Government team testing

Active Indicator Research Phases, Metrics and Milestones

		Phase 1		Phase 2		Phase 3	
	Month	6	12	18	24	30	36
Indicative response metrics	TP rate (R) >	20%	30%	30%	40%	40%	50%
	FP rate <	R/5	R/5	R/10	R/10	R/20	R/20
Detector accuracy metrics	TP rate (R) >	20%	40%	40%	60%	60%	80%
	FP rate <	R/5	R/5	R/10	R/10	R/20	R/20

Summary

- SCITE seeks to
  - Develop methods to model and forecast the performance of alternative configurations of insider threat detection enterprises
  - Discover active indicators that will reliably evoke indicative responses from insiders engaging in espionage

- We are looking for well-executed, creative ideas.

- The BAA supersedes anything presented or said by IARPA at the Proposers' Day.

Questions

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

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Doing Business with IARPA

Mr. Tarek Abboushi

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
  - SCITE BAA: **dni-iarpa-baa-15-09@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-15-09@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 DOD

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

SCITE Program Q&A

Dr. Paul Lehner, Program Manager
IARPA Office for Anticipating Surprise

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)