OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

HECTOR
Proposers' Day Brief

Mark Heiligman
Program Manager

26 July 2017

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)

HECTOR Program Proposers’ Day Agenda

Time	Topic	Speaker
9:00 am – 9:30 am	Registration and Check In	
9:30 am – 9:45 am	IARPA Overview and Remarks	IARPA management
9:45 am – 10:30 am	HECTOR Program Overview	Mark Heiligman Program Manager
10:30 am – 11:00 am	BAA Overview, T&E, GFI/GFE	Mark Heiligman Program Manager
11:00 am – 11:30 am	Break	
11:30 am – 12:00 pm	Doing Business with IARPA	IARPA Acquisition
12:00 pm – 12:30 pm	HECTOR Program Questions & Answers	Mark Heiligman Program Manager
12:30 pm – 1:30 pm	Lunch	
1:30 pm – 3:00 pm	Proposers' 5-minute Capability Presentations	Attendees (**No Government**)
3:00 pm – 4:00 pm	Proposers’ Networking and Teaming Discussions	Attendees (**No Government**)

Proposers’ Day Goals

- Familiarize participants with IARPA and with the HECTOR program concept.
- Solicit feedback and questions.
- Foster networking and discussion of synergistic opportunities and capabilities among potential program participants (A.K.A. “teaming”).
- Please ask questions and make suggestions: this is your chance to influence the design of the program.
  - We appreciate and seek constructive feedback on any / all aspects of the program design and program metrics.
  - Record your questions and comments on the note cards provided and submit them to IARPA staff during the break.
  - After today, questions will be answered in writing on the program website.
- Once a BAA is released, questions can only be submitted to the email address provided in the BAA.

Disclaimer

- These presentations are provided solely for information and planning purposes.
- The Proposers' Day does not constitute a formal solicitation for proposals or abstracts.
- Nothing said at Proposers' Day changes the requirements set forth in a BAA.
  - A BAA supersedes anything presented or said by IARPA at the Proposers' Day.

This briefing is UNCLASSIFIED
All slides are Prepub-Approved

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

IARPA Overview

Dr. Bill Vanderlinde, Chief Scientist

July 2017

IARPA Mission and Method

IARPA's mission is to envision and lead high-risk, high-payoff research that delivers innovative technology for future overwhelming intelligence advantage

- **Bring the best minds to bear on our problems**
  - Full and open competition to the greatest possible extent, funding scientists and engineers in academia and industry, through contracts, grants, OTs, and prize challenges
  - 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 start to finish
  - Run from three to five years
  - Publish peer-reviewed results and data, to the greatest possible extent

IARPA’s Customers

Central Intelligence Agency

Defense Intelligence Agency

Department of State

National Security Agency

Department of Energy

National Geospatial-Intelligence Agency

Department of the Treasury

National Reconnaissance Office

Drug Enforcement Administration

Army

Federal Bureau of Investigation

Navy

Department of Homeland Security

Air Force

Coast Guard

Marine Corps

IARPA Highlights

“One of the government’s most creative agencies.”

– David Brooks, NYT

- Best known for quantum computing, superconducting computing, forecasting tournaments; but our portfolio is diverse -- math, CS, physics, chemistry, biology, neuroscience, linguistics, political science, cognitive psychology. “Everything from AI to Zika.”
- Research highlights include:
  - White House BRAIN Initiative, National Strategic Computing Initiative
  - Nobel Prize for Physics
  - Science “Breakthrough of the Year”
  - MacArthur “Genius”
  - 2,000+ journal articles
- >70% of completed research transitioned to USG partners

nature
MIGHTY ATOMS
A programmable quantum computer based on five atomic qubits PAGES 35 & 63
WE HAVE THE TECHNOLOGY
OFFSHORED POLLUTION
A global solution to the flood of toxic e-waste
MINTING TROUBLE

Current IARPA Research

Collection

- Amon-Hen (space SA)
- FELIX (syn bio)
- FunGCAT (syn bio)
- Ithildin (chem detection)
- HFGeo (HF geolocation)
- MAEGLIN (CBRN)
- MOSAIC (pattern of life)
- Odin (biometrics)
- Proteos (human ID)
- SILMARILS (chem)
- SLiCE (RF tracking)
- UnderWatch (undersea)
- Seedlings and Studies

Analysis

- Aladdin (video search)
- Babel (speech recognition)
- CORE3D (3D modeling)
- DIVA (surveillance video)
- Finder (geolocate images)
- Janus (facial recog)
- KRNS (neuroimaging)
- MATERIAL (translation)
- SHARP (training)
- Seedlings and Studies

Computing

- C3 (cryogenic computing)
- HECTOR (encryption)
- LogiQ (quantum)
- MICrONS (neuromorphic)
- QEO (quantum)
- RAVEN (chip analysis)
- SuperTools (cryogenic)
- TIC (chip security)
- VirtUE (cloud security)
- Seedlings and Studies

Anticipatory Intel

- CAUSE (cyber I&W)
- CREATE (crowdsourcing)
- FUSE (S&T intel)
- Hybrid Forecasting (I&W)
- Mercury (SIGINT I&W)
- SCITE (insider threats)
- Seedlings and Studies

Prize Challenges

- Nail-to-Nail Fingerprinting
- Unconstrained Face Recognition
- Functional Map of the World
- MORGOTH'S CROWN

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 provide opportunities to learn what is coming, and to influence programs
  - **IARPA-Wide BAA "Seedlings"**
    - Typically a 9-12 month study; you can submit your research proposal at any time
    - Strongly encouraged: informal discussion with a PM before proposal submission
  - **Prize Challenges**
    - No proposals required
    - Submit solutions to our problems; if your solutions are the best, you receive a cash prize and bragging rights
  - **Requests for Information (RFIs) and Workshops**
    - Provide input while IARPA is planning new programs

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

HECTOR Program Overview

Mark Heiligman, PM

26 July 2017

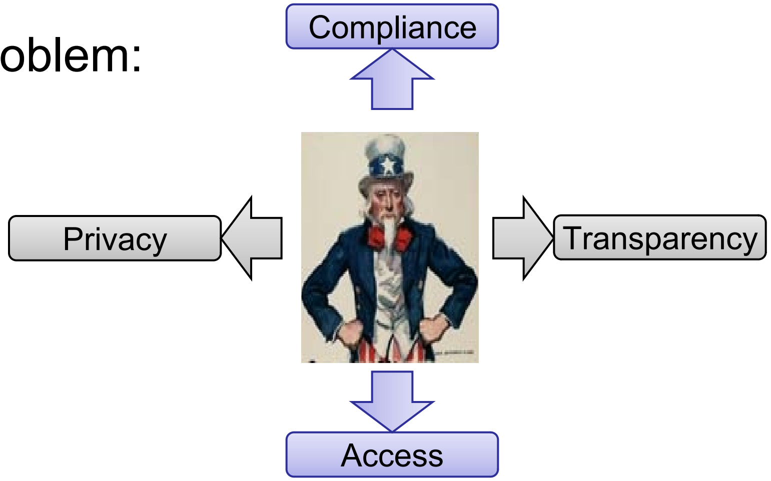
INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)

Presentation Outline

- Motivation and Objectives
- Current Status
- Program Approaches
- BAA Overview
- Program Structure and Deliverables
- Technical Milestones and Program Metrics
- GFI/GFE and Test and Evaluation
- Reporting Requirements
- Schedule
- Management Plan and Teaming
- Eligibility Information
- Proposal Evaluation Criteria
- Program Summary

HECTOR

Problem:



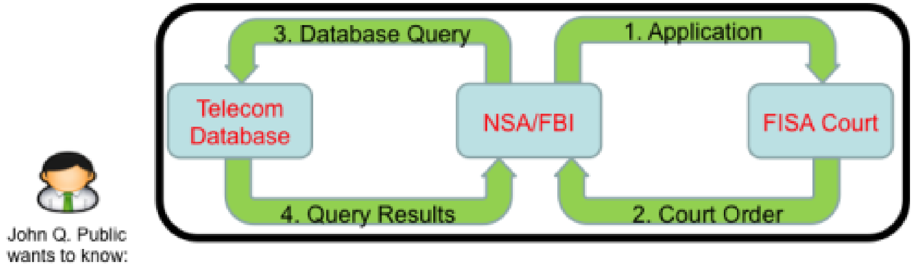
Solution: Expanded Cryptographic Toolset

- Protect Data Under Process
  - Homomorphic Encryption
  - Garbled Circuits
- Functional Encryption
- Zero-Knowledge Proofs
- Verification of Computational Correctness
- Secure Multi-party Computation

Vision: A System Development Platform

- Allows decomposition of distributed systems
- Allows specification/analysis of security properties
- Estimates resource costs of whole systems
- New language allows expression of new concepts
  - Implementation of advanced cryptography
- Verifies implementation of security properties
- Automatically generates verification/auditing tools

Impact: Transform Business Processes



Systems to allow: Mutually distrusting parties,
on untrusted computing platforms,
to collaborate on a shared
computation, for a result that all can trust in.

What are you trying to do?

Transform access control and data protection through advanced cryptography and a holistic approach to systems engineering

Today: Limited cryptographic toolset, and advanced cryptographic techniques are not expressible in today's languages

Systems developed using aggregation, accretion & integration, followed by examining & tweaking the security properties

Security properties of systems are hard to tease out post-development

Future: HECTOR will streamline the development of large-scale distributed systems that make use of advanced cryptographic capabilities

Architects, security experts, designers all have input to the process

Impact: Verifiable systems with trustable outputs in a malicious environment

Exploring and mapping out the new security space

Driving innovation while reducing costs

Why is it Hard?

- Overhead needs to be understood and reduced
  - In FHE, 10^6 per multiplication is widely reported, but orders of magnitude improvements have been seen in recent years
    - Each technology has its own improvement curve, often independent of the others
    - But combining multiple new technologies/concepts together imposes new costs
    - The overall cost to a large system is not obvious
- Newer cryptographic frontiers are poorly understood
    - Particularly the use cases and security/threat models
    - Academic assumptions may not match up to real-world threats
    - Retrofitting new concepts into old languages is a significant challenge
- What are the security implications of design decisions?
    - Need to build realistic systems to solve real-world problems at scale
    - Hard to explain the benefits and issues without a common language

How’s It Done Now?

Security of Data In Transit

Symmetric cryptography was originally invented to protect sensitive data in transit across a hostile environment

Once decrypted, data protection would be lost

The Evolution of Cryptography

Security of Data In Transit

Asymmetric cryptography allowed communicants to “go secure” from an insecure state, and to authenticate the source of a message.

Authentication of Data Source

The Evolution of Cryptography

Security of Data In Transit

Cryptographic hashing and key derivation allowed for true protection of data at rest.

Authentication of Data Source

Security of Data At Rest

Unfortunately, once a device is unlocked, just as for data in transit, any data protection is lost.

Next Steps in Cryptography

Security of Data In Transit

Authentication of Data Source

Cryptographic computing techniques allow data to be processed without revealing its nature.

They allow fine-grained access control to the data itself and to the ability to perform computations on the data.

There is no loss of control.

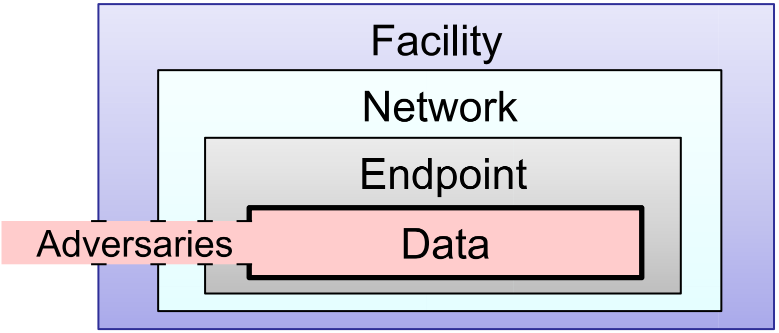
Security of Data At Rest

Security of Data In Process

Limitations of Present Approaches

Today's access control paradigm:

After each boundary failed
we added another boundary
without really fixing anything



- Currently no other way to protect data under process
  - Advanced crypto limited to academia and some pilots
  - Languages support at best one new concept at a time
  - Overhead costs decreasing, but still potentially prohibitive

State-of-the-art Cryptography

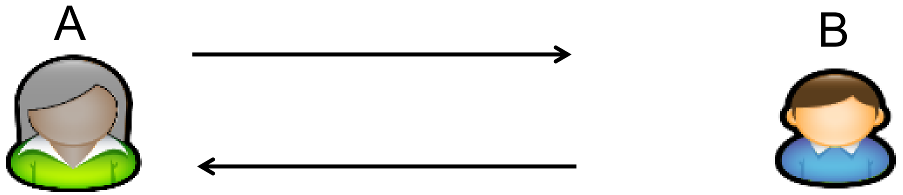
- Advanced technologies change the nature of computation:
  - Fully / Somewhat / Partial Homomorphic Encryption
  - Verifiable Computing
  - Functional Encryption
    - Conditional Proxy Re-encryption
  - Zero-Knowledge Proofs
  - Oblivious RAM
  - Secure Multiparty Computation
    - Oblivious transfer, Multiparty circuit evaluation
    - Private Set Intersection
    - Private Information Retrieval
- Many of these can be brought into the mainstream

See the Technology Primer slides for more details

Census Data Processing and Trade Space Evaluation

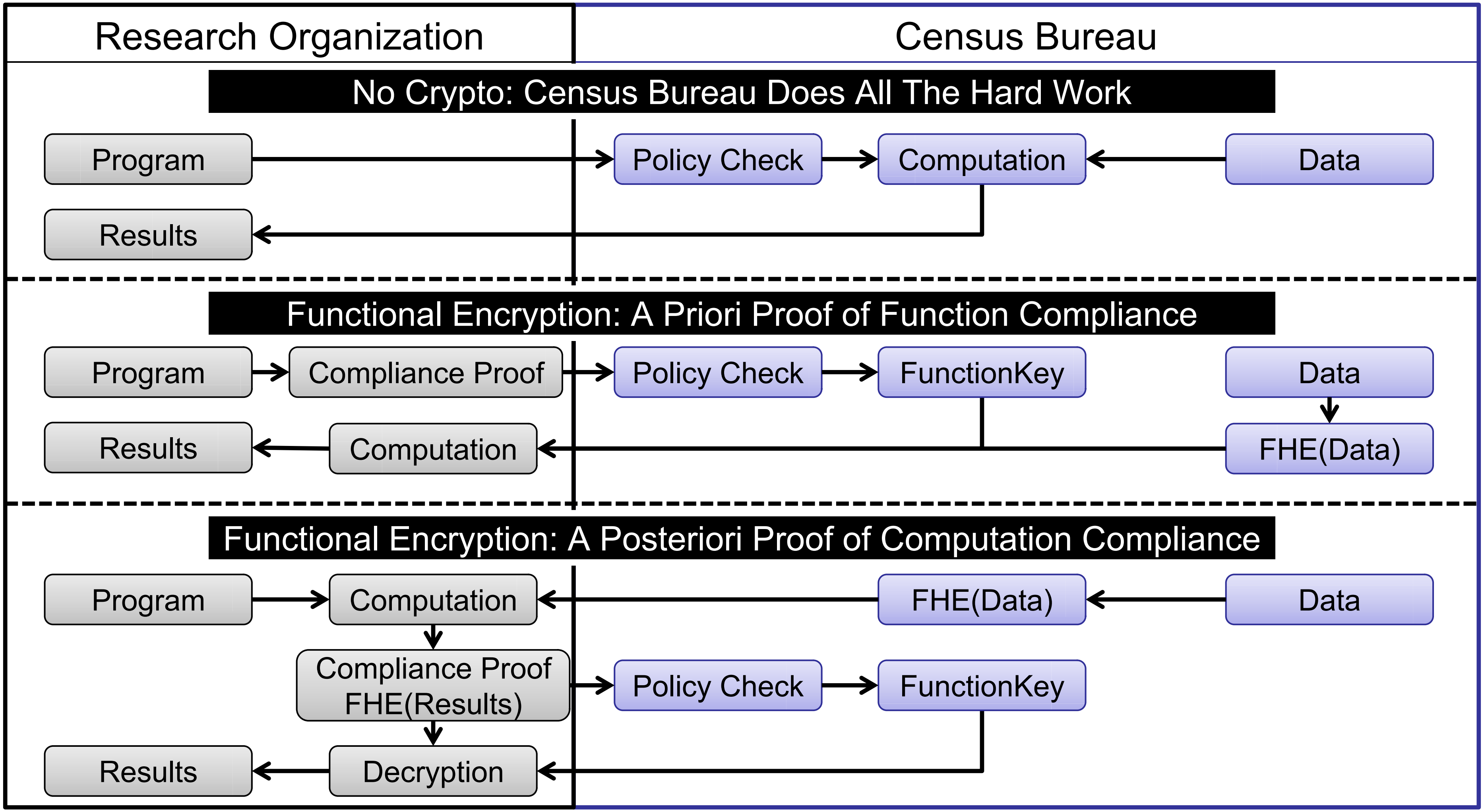
EXAMPLE CHALLENGE #1

Census Data



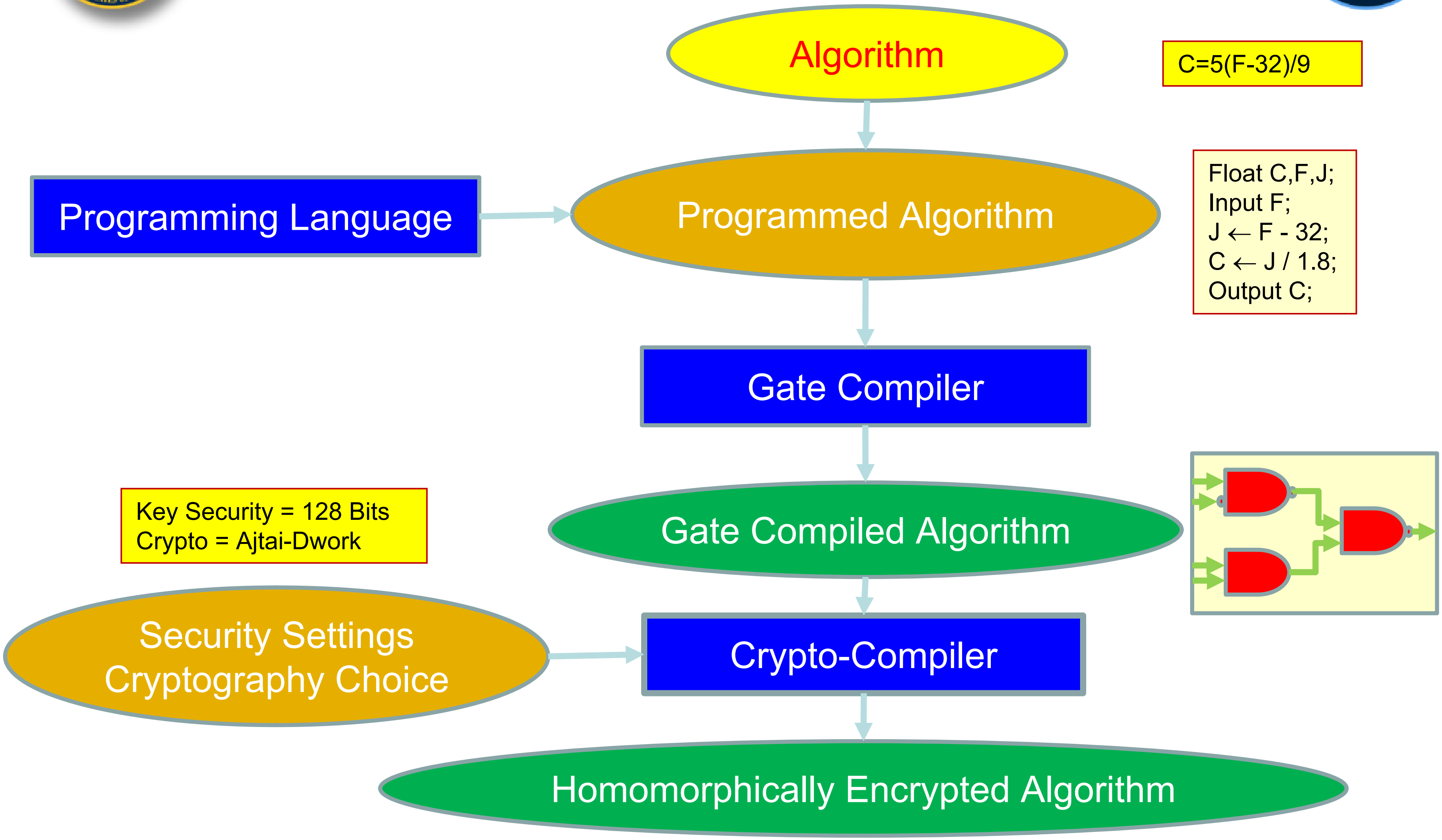
- Case: A researcher wants to perform computations on sensitive PII data held by the census bureau to get aggregate results
- Homomorphic Encryption: Bob provides the data in an encrypted form. Alice performs complex computations on the encrypted data, and sends the encrypted result to Bob
- Bob decrypts the result and returns the unencrypted answer to Alice
- Verification: Bob need to verify that the computation that Alice claims to have performed is actually the computation that Alice did perform. Bob needs to check that the computation was in conformance with policy.

One Problem, Numerous Solutions



Questions and Issues

- Example: Functional Encryption
  - The capability can be described very simply
    - I give you data, but you can only evaluate functions that I authorize you to compute
  - However, the underlying mechanism is inherently complicated
  - The security implications are also inherently complex
  - How accessible can we make the language syntax / security reports?
    - You can no longer simply “call” a function – there is an authorization process
  - Functional encryption is expensive
    - Are there theoretical lower limits to the overhead?
    - When integrated into a large system is this still a bottleneck?
  - Leakage is Poorly Understood
- Similar questions and issues apply to other techniques



Algorithm

C=5(F-32)/9

Programming Language

Programmed Algorithm

```
Float C,F,J;
Input F;
J ← F - 32;
C ← J / 1.8;
Output C;
```

Gate Compiler

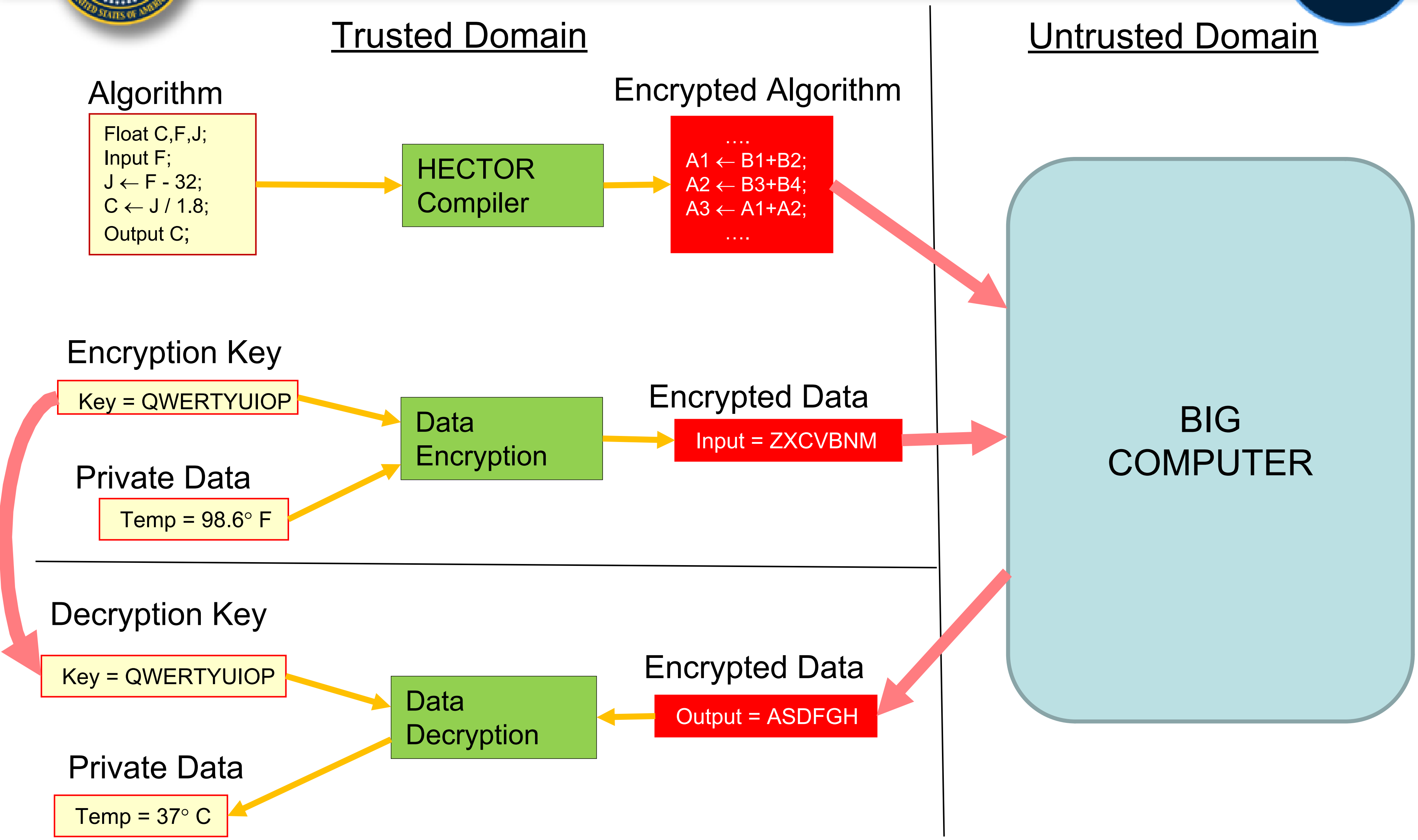
Key Security = 128 Bits
Crypto = Ajtai-Dwork

Gate Compiled Algorithm

Security Settings
Cryptography Choice

Crypto-Compiler

Homomorphically Encrypted Algorithm



Trusted Domain

Untrusted Domain

Algorithm

```
Float C,F,J;
Input F;
J ← F - 32;
C ← J / 1.8;
Output C;
```

HECTOR Compiler

Encrypted Algorithm

```
….
A1 ← B1+B2;
A2 ← B3+B4;
A3 ← A1+A2;
….
```

BIG COMPUTER

Encryption Key

Key = QWERTYUIOP

Data Encryption

Private Data

Temp = 98.6° F

Encrypted Data

Input = ZXCVBNM

Decryption Key

Key = QWERTYUIOP

Data Decryption

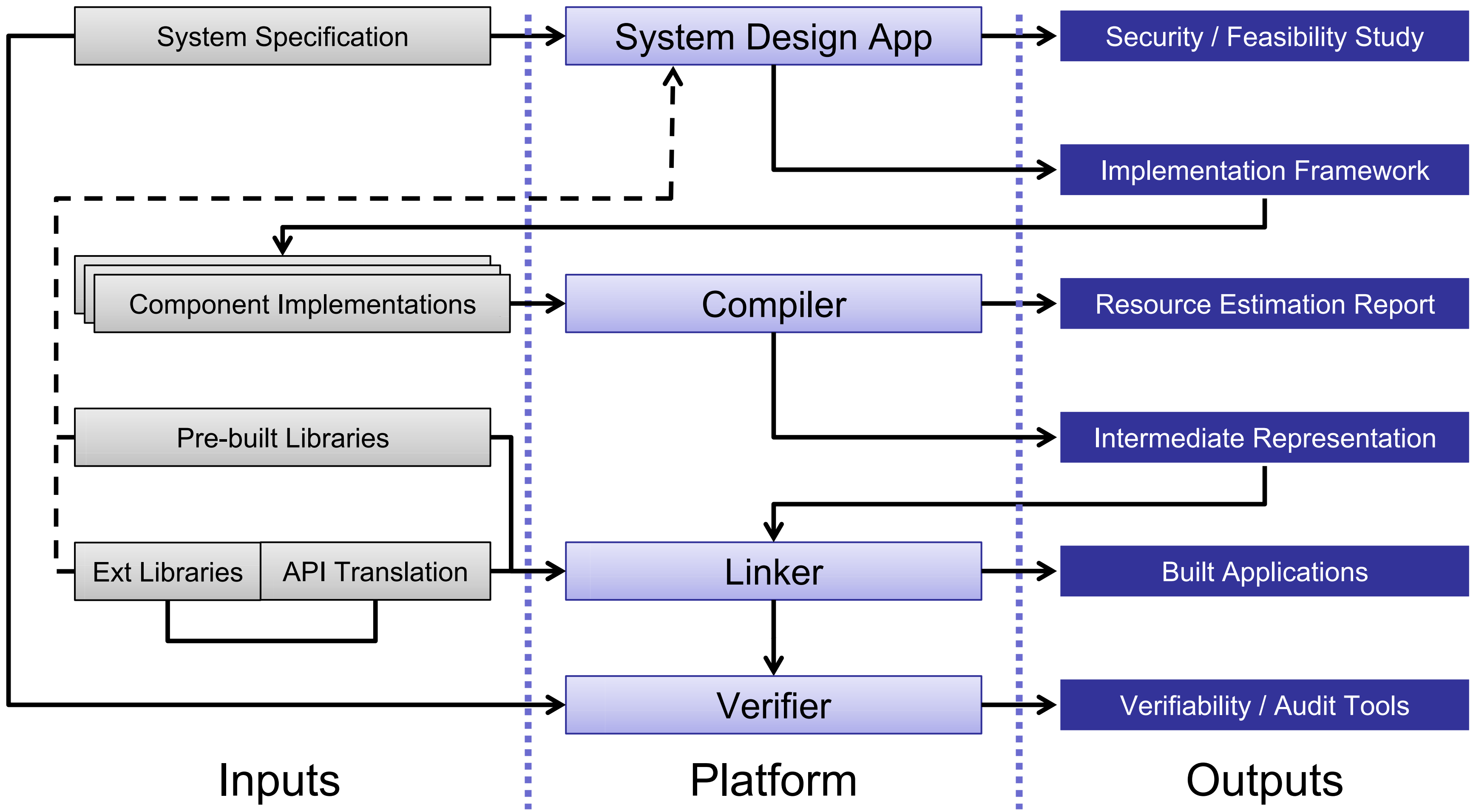
Encrypted Data

Output = ASDFGH

Private Data

Temp = 37° C

System Development Platform



What is new about HECTOR?

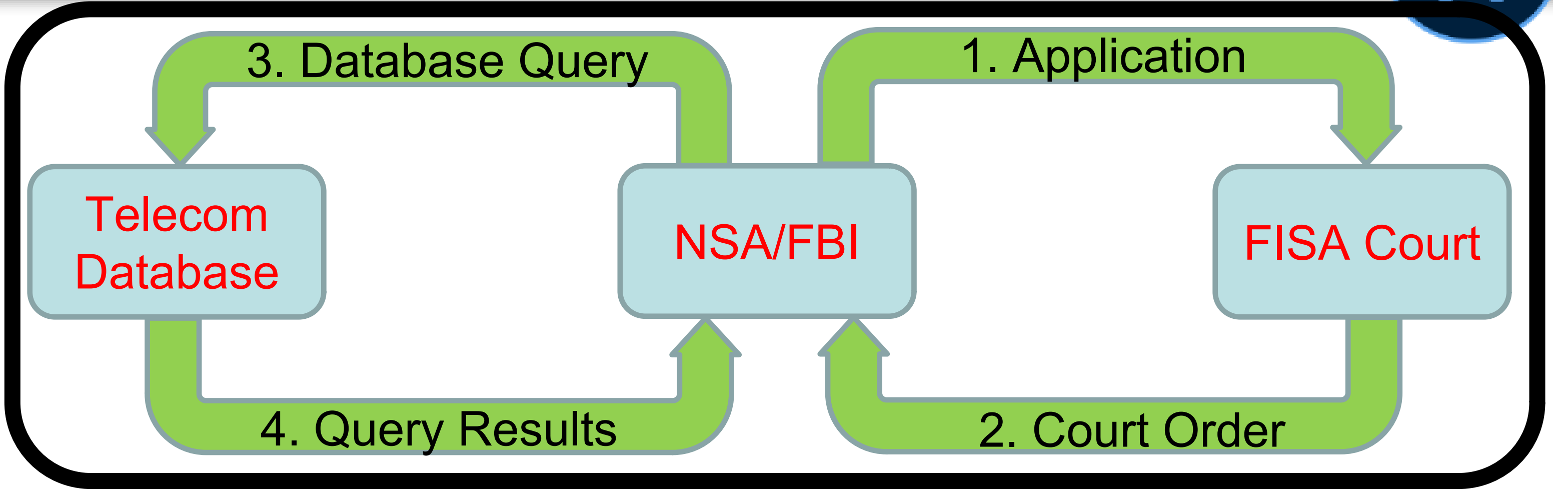
- Automation of flow-down design process
  - Requirements & constraints automatically verified
  - Functional decomposition of distributed systems
  - Performs resource estimation & identifies bottlenecks
  - Distills input from domain experts
    - System goals, security requirements and threat environment are expressed once and drive system requirements and constraints
    - If any of these change, the system design can be reassessed
  - Advanced crypto concepts are abstracted away
    - The capabilities they provide are built into an extensible language
    - The composition of multiple concepts is supported by language

What difference will HECTOR make?

- Reduce costs and risks associated with secure IC systems
  - An up-front assessments of the resource costs
  - Enable verifiable regulatory compliance, greater partner collaboration

- Deliver the infrastructure and tools to simplify security
  - Cryptographic implementations can be re-used in different contexts
  - Calculates security implications of architectural & design decisions
  - Enables system certifiers to have an automated assurance of correctness, possibly for the most critical aspect of a system

- Empower system architects and software developers
  - Know what resources are required to get the job done
  - Intuitively develop secure large-scale distributed systems



John Q. Public wants to know:

1. Does the FISA application conform to policy and law?

   Need to verify compliance with policy without compromising the content of the application.

   a) Encrypt FISA court application.
   b) Homomorphically compute whether the application is policy compliant.

2. Is the FISA court applying the law correctly?

   Need to verify that the FISA court order is limited to what was applied for.

   a) FISA court issues warrant in the form of a function key to allow a specific computation.
   b) Homomorphically compute whether the computation being warranted corresponds to the what was applied for.

3. Is the database search being done correctly?

   Need to verify that the function was applied correctly.

   a) Perform functional verification

4. Are the returns from the database search correct and are they legally compliant?

   Need to confirm that the results conform to policy and law.

   a) Homomorphically compute whether the encrypted return is legally compliant

BAA Overview, T&E, GFI/GFE

BAA Highlights

- Three core focus areas
  1. System Development Platform
  2. Programming Languages / Representation Formats
  3. Cryptographic Protocols and Optimization

- Three phases: Plan & Design, Implement, Optimize/Refine

- Program Duration: Five Years

- Performers will demonstrate exemplar applications:
  - Initial challenge problems declared at start of program
  - Some challenge problems defined by performers themselves

Core Focus Areas

System Development Platform

- Overview
  - The goal of the system development platform focus area is to implement a full suite of development tools for secure, distributed applications.
  - Most of the use cases targeted by the HECTOR program are inherently multi-party, which could include distributed development and verification of security-critical aspects of the system.

Core Focus Areas

Programming Languages / Representation Formats

- Overview
  - The goal of this focus area is to develop and document a number of programming languages and representation formats needed by the HECTOR program, to develop exemplar applications that use these languages / formats to meet challenge problems, and to interface both with other focus areas within a performer team and with other performer teams with respect to standardization.
  - One of the goals of HECTOR is the development of a component implementation language that allows for the intuitive expression of advanced cryptographic techniques, and that allows for future expansion of its conceptual scope as new techniques are developed.
  - Each offeror is expected to develop their own component implementation language, which should be a full programming language that provides an extremely high level of abstraction around key management concepts and cryptographic operations.

Core Focus Areas

Cryptographic Protocols and Optimization Focus Area

- Overview
  - The goal of this focus area is to implement or adapt existing cryptographic protocols so that they can be used within the system development platform in an interchangeable and composable fashion, and to explore performance improvements.

Collaboration and Standardization

- While offerors are expected to develop their own unique tools and programming languages, and research and develop their own optimizations to cryptographic protocols, two key aspects of the HECTOR program would benefit from standardization, and offerors will be expected to collaborate on a single common solution in those areas.
- One goal of HECTOR is to encourage standardization at the intermediate representation level, so offerors will be expected to collaborate on a common representation language, with coordination from the T&E team.
- Offerors will also be expected to collaborate on a common standard module format for incorporating implementations of cryptographic protocols.

Program Structure: Phase I

Phase I: Planning and Design

- Overview
    - The goal of Phase 1 is to allow performers to demonstrate the viability of their plans and develop a solid system design.
    - During Phase I, performers will develop detailed plans, designs, and specifications, and build automated grammar and syntax checkers for any programming languages or representation formats developed during the year.

Program Structure: Phase I

Phase I: Plan and Design

- Details
  - Implement GFI-specified protocols/schemes selected to match challenge problems, and perform initial baselining.
  - Develop a detailed research plan for novel secure data services, to include cryptographic computing concepts, schemes, and/or protocols.
  - Develop detailed specification documents and initial syntax checker utilities for performer-specific programming languages and representation formats.
  - Collaboratively develop detailed specification documents for common standards to include the intermediate representation language and the metadata-rich module format.
  - Develop syntax/format checker utilities for the intermediate representation language and the metadata-rich module format.
  - Develop a detailed software design document for the tools, to be developed in Phase II, that together form the system development platform.
  - Develop exemplar application source artifacts to show how their programming languages and representation formats would be used to solve challenge problems associated with Phase I.

Program Structure: Phase II

Phase II: Implement

- Overview
  - The goal of Phase II is to implement and demonstrate the full capabilities of the system development platform.
  - Delivered software is expected to be “research-grade” rather than “production-grade” but must be fully documented, and capable of operating on and building applications for consumer-level computing hardware and operating systems.

Program Structure: Phase II

Phase II: Implement

- Details
  - Research new concepts for secure data services.
  - Research performance improvements in existing secure data services.
  - Implement additional secure data services.
  - Implement all system development platform functionality and tools.
  - Develop exemplar applications to answer the challenge problems for Phase II.

Program Structure: Phase III

Phase III: Optimize and Refine

- Overview
  - The goal of Phase III is to optimize and further increase the capabilities of the system development platform, both in terms of its performance as a tool, and in terms of the performance of the applications it can generate.
  - To test the extensibility of the programming languages’ conceptual scope, a new cryptographic computing concept will be introduced at the start of Phase III, selected from those proposed by the performers and the test and evaluation team in Phase II.
  - Each performer will be expected to demonstrate the inclusion of this new concept into their programming language, and its mapping to functionality at the intermediate representation level.

Program Structure: Phase III

Phase III: Optimize and Refine

- Details
  - Research and/or implement performance improvements in existing secure data services.
  - Implement additional secure data services.
  - Incorporate optimization strategies into the compiler.
  - Improve the accuracy and/or performance of resource estimation tools.
  - Develop exemplar applications to answer the challenge problems for Phase III.

Out of Scope

- Cryptanalysis of the cryptographic protocols / schemes, in particular cryptanalytic research into the hardness of properties labeled as hardness assumptions.
- Acquisition of high performance computers or equivalent hardware.
- Resource or security improvements that rely on trusted hardware.
- Development of special purpose hardware.

HECTOR Deliverables

- Languages / Representation Formats
  - Concept-Extensible Application Implementation Language
  - Annotated System Architecture Description Language
  - Threat Model / Security Model for Reasoning Engine
  - Intermediate Representation Language
  - Metadata-Rich Linkable Module Format
- Tools
  - System Design Tool
  - Reasoning Engine for Security/Feasibility Studies
  - Compiler + Linker
  - Resource Estimator for Cryptographic Systems
  - Automated Verifier / Verification Tool Generator
- Advances in Cryptographic Frontiers
  - Implementations of New/Existing Schemes and Protocols
  - New Concepts for Cryptographic Computing
  - Efficiency Improvements for Existing Concepts

Phase 1 HECTOR Deliverables

Date	Event / Deliverable
	Program Phase I
Month 1	Program Kick-off Meeting
Month 3-4	Annual Site Visits (Year 1)
Month 6	Technical Exchange Meeting (TX1) First exchange on common standards
Month 10	Annual Principal Investigators (PI) Program Review Meeting (Year 1) Second exchange on common standards
Month 12	Performers deliver Month-12 Deliverables and Annual Research Report Concept-Extensible Application Implementation Language Annotated System Architecture Description Language Threat Model / Security Model Format for Reasoning Engine Intermediate Representation Language Metadata-Rich Linkable Module Format Syntax checkers for each format/language listed above Software design document for system development platform Implementation of GFI-specified Phase I secure data services Phase I Challenge Problem Implementations Detailed research plan
Month 12	Phase I Final Report

Phase 2 HECTOR Deliverables

Date	Event / Deliverable
	Program Phase II
Month 13	Program Phase II Kick-off Meeting Third exchange on common standards
Month 14	Technical Exchange Meeting (TX2)
Month 15-16	Annual Site Visits (Year 2)
Month 18	Technical Exchange Meeting (TX3)
Month 22	Annual PI Program Review Meeting (Year 2)
Month 30	Technical Exchange Meeting (TX4)
Month 34	Annual PI Program Review Meeting (Year 3)
Month 36	Performers deliver Month-36 Deliverables and Annual Research Report System Development Platform, Version 1 Implementation of GFI-specified Phase II secure data services User guides and documentation Phase II Challenge Problem Implementations
Month 36	Phase II Final Report

Phase 3 HECTOR Deliverables

Date	Event / Deliverable
	Program Phase III
Month 37	Program Phase III Kick-off Meeting Forth exchange on common standards
Month 39	Technical Exchange Meeting (TX5)
Month 40-41	Annual Site Visits (Year 4)
Month 44	Technical Exchange Meeting (TX3)
Month 46	Annual PI Program Review Meeting (Year 4)
Month 50	Technical Exchange Meeting (TX4)
Month 58	Annual PI Program Review Meeting (Year 3)
Month 60	Performers deliver Month-60 Deliverables and Annual Research Report System Development Platform, Version 2 Implementation of GFI-specified Phase III secure data services Phase III Challenge Problem Implementations
Month 60	Phase III Final Report

Definitions of Program Metrics - Services

Area	Secure Data Services Metrics and Methodology
Novel Secure Data Services	Number of well-defined new services specified; soundness verified by peer review within program (P/F); associated overhead (time, number of operations).
Implementation of Secure Data Service Schemes	Number correctly implemented; correctness verified by T&E (P/F), Processing overhead

Definitions of Program Metrics - Languages

Area	Language Metrics and Methodology
Language Specification	Measure range + ease of expression by making performers implement 20 unseen test problems (simple routines) in 1 month at end of year Use syntax checker; T&E evaluate ease of comprehension Measure # of correctly specified solutions, # lines of code

Definitions of Program Metrics - Toolchain

Toolchain Output	Toolchain Metrics and Methodology
Security/Feasibility Study	Number of security models for which accurate results are given – verified by test vectors
Auto-generated design level artifacts	System complexity that can be accurately handled – Number of manually verified mini-challenge problems.
Intermediate Representation	Completeness measured by mini-challenge problems Parsers / syntax checkers from performers should agree
Resource Estimations	Accuracy of resource estimates, number of relevant quantities that can be estimated, all verified manually using mini-challenge problems, Efficiency of estimation (Time)
Compiler	Independent verification of formal proof of correctness of compiler functionality, where provided; correctness of IR output – verified using mini-challenge problems, or for larger problems by observing application in action
Generated Application	Correctness of implementation – verified by test harness, live demonstration, test vectors and/or proof of correctness (P/F)

Phase 1 Planned Milestones

Area	Phase I Entry	Phase I Milestones
Secure Data Services	GFI Scheme list	Implementation of all GFI-specified schemes selected to match challenge problems; Initial baseline estimates of resource requirements..
	Basic research plan	Detailed research plan for novel secure data services: concepts/schemes/protocols
Language	System specification language	System specification language / representation format specification document
	Outline of language	Implementation programming language specification, including FHE, SMC, functional encryption
	GFI problem list	Three GFI programming challenge problems (algorithms) & 10 performer/T&E generated test routines implemented in language
	Ideas for IR	Intermediate representation format specification
Toolchain	Basic syntax checker design	Automated syntax checkers for all new languages / representation formats
	Linker concepts	Linkable library module format specification
	Software design concepts	Detailed software design document

Phase 2 Planned Milestones

Area	Phase II Entry	Phase II Milestones
Secure Data Services	GFI Scheme list	Implementation/baselining of full set of interconnected secure data services; Improvement of isolated protocols (10x)
	Detailed research plan	Novel secure data services concept/scheme research report: how they connect with existing schemes
Language	Language and format specifications	Refined language / format specifications due to implementation constraints
	Implementation language	Enhanced implementation language specification to add verifiable/transparent/auditable computation
	Specifications	Full documentation for all formats and languages
	GFI problem list	All GFI programming challenge problems (algorithms) and performer/T&E generated routines implemented
Toolchain	Syntax checkers	Compilers and other toolchain artifacts implemented
	Linkable module format	Linkable modules derived from secure data services
	Software design document	Demonstration of toolchain compiling / verifying Phase 1 GFI challenge problems

Phase 3 Planned Milestones

Area	Phase III Entry	Phase III Milestones
Secure Data Services	Implementation of optimized GFI-specified schemes	Demonstrated efficiency improvements (10x in interconnected schemes, 100x in isolated schemes)
	All new performer concepts / schemes	Implementation of secure data service concepts / schemes / protocols from own and/or other performer research
Language	Refined language / format specifications	Enhanced implementation language to add at least one new concept from program research results
	Full documentation	Full language documentation including at least one new concept
	All GFI challenge problems implemented	3 selected additional performer-suggested programming challenge problems (algorithms) implemented in language
Toolchain	Toolchain implemented	Implementation of at least one new language concept in toolchain
		Optimization of toolchain performance (2x)
		Implementation of optimizing compiler within toolchain

Measurement of Success

Challenge Problems	Test & Evaluation
GFI challenges from real-world problems Can exercise entire toolchain See implementation of new concepts "Chinese menu" maximizes breadth	Use existing metrics & techniques for: Language acceptability criteria Assessing representation formats Testing complier toolchains
Performer generated challenge problems Demonstrate range of expression Require "future-proof" software	Toolchain output allows review of Automated security analyses Resource estimation capabilities

Pick Your Technologies	Pick a Problem	Pick the Adversaries
Functional Encryption	Census Data Processing	Malicious
Verifiable Computation	Health Record Processing	Honest But Curious
Oblivious RAM	Sealed Auctions	Covert Malicious

Program Roles and Responsibilities

- **Performers**
  - Research & Development
- **Government Support**
  - Government Furnished Information (GFI):
    - Challenge problems
    - At the kickoff of each program phase, the Government will provide performers with a list of benchmarks and background information as GFI
  - Government Furnished Equipment (GFE):
    - None
  - Testing and Evaluation:
    - Metrics for evaluation
    - Yearly report on performer progress so far
    - Quarterly cross-performer meetings per focus area

Government Furnished Information (GFI)

- The followings are examples of GFI:
  - Secure data services to be implemented by performers, including full specification or reference to same
  - Specification of micro-scale challenge problems to be used to demonstrate the correct operation of tools.
  - Specification of large-scale challenge problems to be used to demonstrate the application of the system development platform to real-world problems.

Challenge Problems

- The HECTOR program will use a variety of challenge problems to allow performers to demonstrate the merits of their programming languages and representation formats, and to demonstrate the successful operation of their system development platform

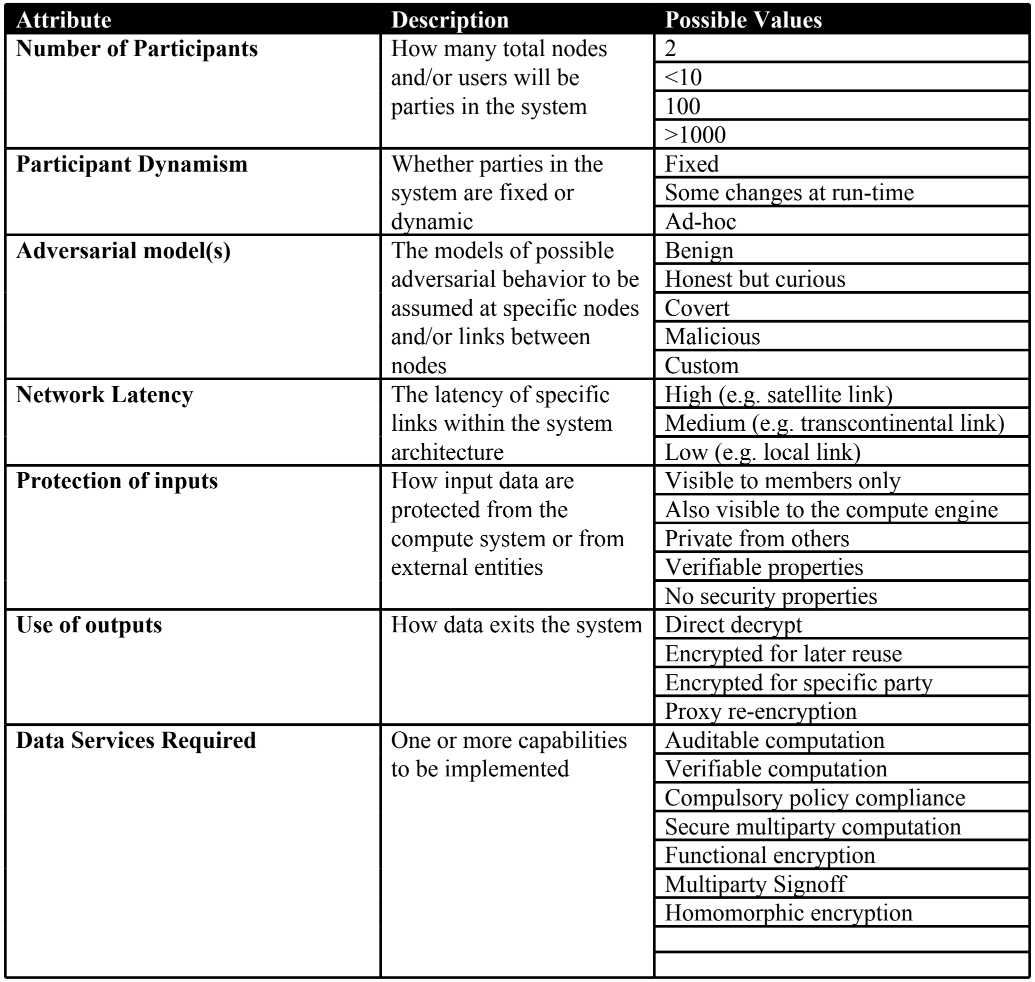
- Challenge problems will be provided as Government Furnished Information (GFI) at the outset of each phase. Initial challenge problems will be provided at program kickoff.

Example Applications
Sealed Auction
Treaty Negotiation
Policy-compliant data processing
Outsourced data processing
Secure Election

Challenge Problems

- Challenge problems will be given in two varieties: small-scale challenges such as invoking a specific secure data service, and system-scale challenges such as implementing an entire secure data processing system.
- The system-scale challenges will be picked from a “menu” of possibilities through which multiple paths can be generated by selecting different attributes at each stage of the menu.
- A preliminary list of menu items is provided in the next chart.

Challenge Problems – Menu Items



Attribute	Description	Possible Values
Number of Participants	How many total nodes and/or users will be parties in the system	2
		<10
		100
		>1000
Participant Dynamism	Whether parties in the system are fixed or dynamic	Fixed
		Some changes at run-time
		Ad-hoc
Adversarial model(s)	The models of possible adversarial behavior to be assumed at specific nodes and/or links between nodes	Benign
		Honest but curious
		Covert
		Malicious
		Custom
Network Latency	The latency of specific links within the system architecture	High (e.g. satellite link)
		Medium (e.g. transcontinental link)
		Low (e.g. local link)
Protection of inputs	How input data are protected from the compute system or from external entities	Visible to members only
		Also visible to the compute engine
		Private from others
		Verifiable properties
		No security properties
Use of outputs	How data exits the system	Direct decrypt
		Encrypted for later reuse
		Encrypted for specific party
		Proxy re-encryption
Data Services Required	One or more capabilities to be implemented	Auditable computation
		Verifiable computation
		Compulsory policy compliance
		Secure multiparty computation
		Functional encryption
		Multiparty Signoff
		Homomorphic encryption

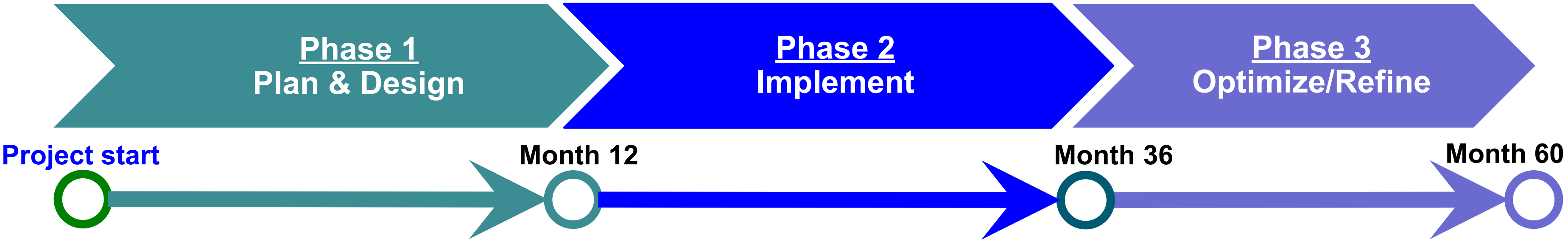
T&E Team Roles and Responsibilities

- Multidisciplinary T&E team draws from multiple sources
    - SETA: oversight and reporting
    - FFRDC: cryptographic expertise
    - Academia: compiler design
    - Industry: large scale software design, system specifications

Risks

- Excessive Overhead
  - We do not know whether the known overheads of advanced cryptographic techniques will still be excessively onerous when incorporated into the system as a whole
  - Mitigation: if HECTOR cannot bring those overheads down, it can at least identify bottlenecks at the system level and show what could be achieved with a specific further reduction
- Automated Security Analysis
  - While the system specification format should ease the process, flexible representation of system goals and security threats to generate a thorough and meaningful automated security analysis is currently an unsolved problem
  - Mitigation: by forcing up-front declaration of these system properties, HECTOR will at least ease any subsequent manual analysis

HECTOR Timeline



Phase 1
Plan & Design

Phase 2
Implement

Phase 3
Optimize/Refine

Project start

Month 12

Month 36

Month 60

- Develop detailed plans, designs, and specifications, and build automated grammar and syntax checkers.
- Demonstrate viability of plans and system designs.

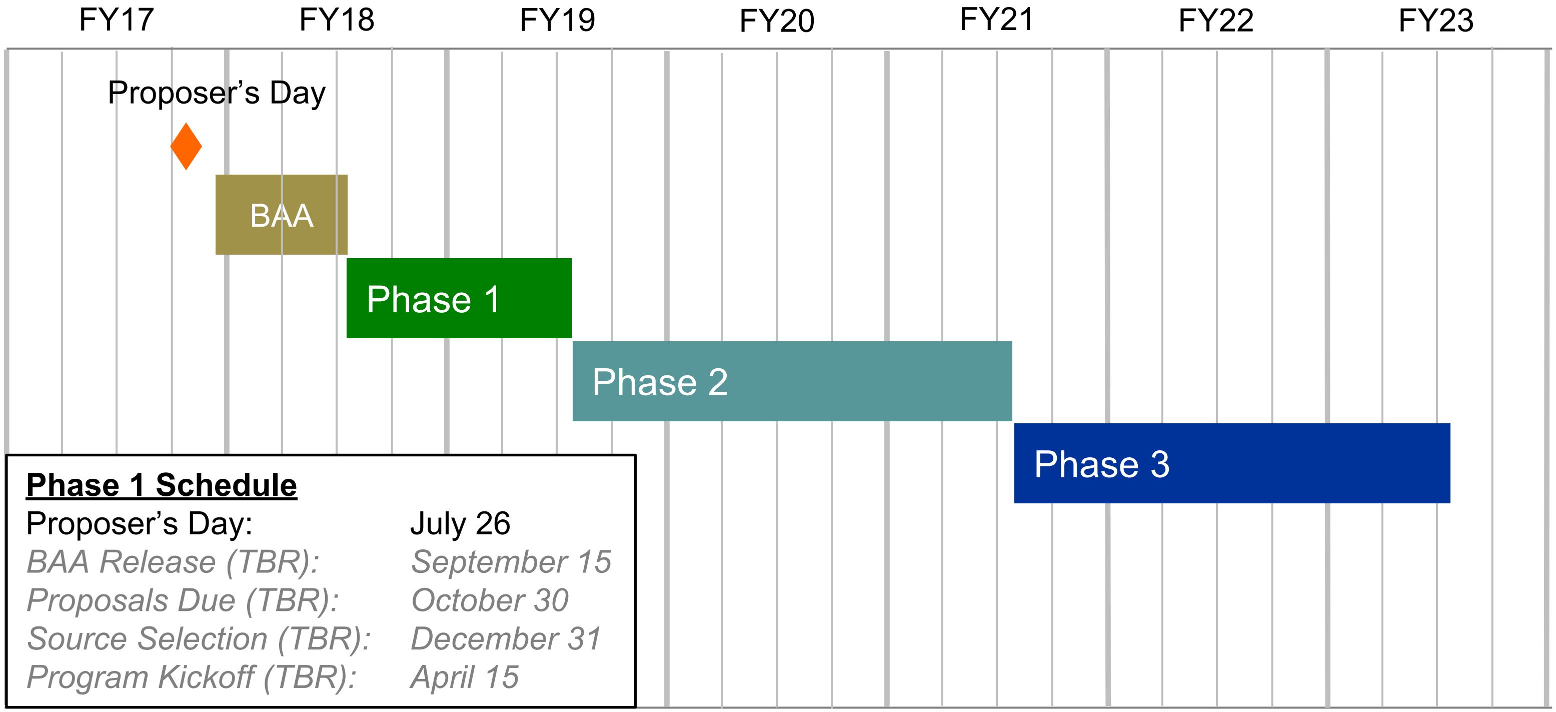
- Research new concepts for secure data services & performance improvements in existing services.
- Implement additional secure data services.
- Implement all system development platform functionality and tools.
- Develop exemplar applications to address the challenge problems.

- Research & implement performance improvements and additional secure data services.
- Incorporate optimization strategies.
- Improve the accuracy & performance of resource estimation tools.
- Develop exemplar applications to address the challenge problems.

Reporting Requirements

- Monthly technical report – highlight progress from past month and plans for next month.
- Monthly financial report – form will be provided.
- Program kick-off meeting – first month of program.
- Annual performer site visit – beginning of each program year.
- Technical Exchange Meetings.
- Semi-annual Program Review Meetings.
- Test Plans
- Reports – submitted at the end of each year.

Notional/Target Schedule



Phase 1 Schedule

Proposer's Day:	July 26
BAA Release (TBR):	*September 15*
Proposals Due (TBR):	*October 30*
Source Selection (TBR):	*December 31*
Program Kickoff (TBR):	*April 15*

BAA & Review and Source Selection

Management Plan and Teaming

- Depth and diversity will be essential to accomplish the many challenges in tool development and extension.
  - Scalability and Optimization
    - Make sure you have enough people, both from industry and academia to accomplish the goal and from proof-of-concept to large scale.
    - Sufficient resources to follow critical path while still exploring new approaches.
  - Completeness – teams should not lack any capability necessary for success, e.g. should not rely upon results or enabling technology from the community at large.
  - Tightly knit teams:
    - Clear, strong management; single point of contact.
    - No loose confederations; No teaming for teaming's sake.
    - Each team member should contribute significantly to the program goals.
  - Team members not required to participate all 5 years – consider phase transitions.

Proposal Evaluation Criteria

- Evaluation criteria in descending order of importance are:
  - Overall technical merit,
  - Effectiveness of proposed work plan,
  - Relevance to IARPA mission and HECTOR program goals,
  - Relevant experience and expertise of the members of the team,
  - Cost realism.
- All responsive proposals will be evaluated by a board of qualified government reviewers.

Point of Contact

Dr. Mark I. Heiligman

Program Manager

IARPA, Office of the Director of National Intelligence

Intelligence Advanced Research Projects Activity

Washington, DC 20511

Phone: (301) 851-7432

Fax: (301) 851-7672

Electronic mail: dni-iarpa-baa-17-05@iarpa.gov

(include IARPA-BAA-17-05 in the Subject Line)

Website: www.iarpa.gov

Questions? Please fill out cards.

Questions?

Eligibility Information

- Collaborative efforts are strongly encouraged.
  - Content, communications, networking and team formation is the responsibility of proposers.
- Foreign organizations and/or individuals are welcome to participate.
  - Must comply with Non-Disclosure Agreements, Security Regulations, Export Control Laws, etc., as appropriate.
- 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.
- Please notify the HECTOR Program Manager ASAP if you wish to utilize any resources from these organizations.
  - If IARPA determines that the resources are unique and do not exist in the private sector, IARPA will attempt to work directly with that organization to arrange for that capability to be made available to all program participants who might benefit.

Doing Business with IARPA

Mark Heiligman
Intelligence Advanced Research Projects Activity

Office of the Director of National Intelligence
IARPA
BE THE FUTURE

HECTOR Proposers’ Day Agenda

Time	Topic	Speaker
9:00 am – 9:30 am	Registration and Check In	
9:30 am – 9:45 am	IARPA Overview and Remarks	IARPA management
9:45 am – 10:30 am	HECTOR Program Overview	Mark Heiligman Program Manager
10:30 am – 11:00 am	BAA Overview, T&E, GFI/GFE	Mark Heiligman Program Manager
11:00 am – 11:30 am	Break	
11:30 am – 12:00 pm	Doing Business with IARPA	IARPA Acquisition
12:00 pm – 12:30 pm	HECTOR Program Questions & Answers	Mark Heiligman Program Manager
12:30 pm – 1:30 pm	Lunch	
1:30 pm – 3:00 pm	Proposers' 5-minute Capability Presentations	Attendees (**No Government**)
3:00 pm – 4:00 pm	Proposers’ Networking and Teaming Discussions	Attendees (**No Government**)

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 (Proposal & Submission Information)
- Read Frequently Asked Questions on the IARPA @

  http://www.iarpa.gov/index.php/faqs
- Send your questions as soon as possible
  - HECTOR BAA: **dni-iarpa-baa-17-05@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 <u>not</u> 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
- Exception to GPR
  - State in the proposal any restrictions on deliverables relating to existing materials (data, software, tools, etc.)

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
  - IARPA PM decides on approval for release or receiving courtesy copy

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 and subcontractors 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 a 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-17-05@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.

Point of Contact

Dr. Mark I. Heiligman

Program Manager

IARPA, Office of the Director of National Intelligence

Intelligence Advanced Research Projects Activity

Washington, DC 20511

Phone: (301) 851-7432

Fax: (301) 851-7672

Electronic mail: dni-iarpa-baa-17-05@iarpa.gov

(include IARPA-BAA-17-05 in the Subject Line)

Website: www.iarpa.gov

Questions? Please fill out cards.