



IWTSD INDUSTRY DAY

IWTSD Overview

March 6, 2025

Identify and develop capabilities for DoD to conduct Irregular Warfare against all adversaries, including Great Power competitors and non-state actors, and to deliver those capabilities to DoD components and interagency partners through rapid research and development, advanced studies and technical innovation, and provision of support to U.S. military operations.

Objectives:

- Support the National Defense Strategy and the Annex for Irregular Warfare.
- Provide forums to solicit and collaborate on R&D requirements.
- Rapidly advance technology development, deliver prototypes for operational tests and evaluations, and assist in product transition.
- Promulgate technology & information exchange.
- Influence policy – identify enablers.



ORGANIZATION

Executive Program Direction

DoD
OASD(SO/LIC) SSO

Program Management

Irregular Warfare Technical Support Directorate (IWTSD)

Subgroups and Chairs

Advanced Analytics

USSOCOM CDAO

Chemical, Biological, Radiological, Nuclear, and Explosives

JPEO CBRND / FBI / DHS S&T

Expeditionary Force Protection

OPMG / DOE / FBI

Explosive Ordnance Disposal and Explosive Operations

JSEOD / NBSCAB / CEHC

Human Performance and Training

Influence and Information Capabilities

USASOC

Protection, Survivability, and Recovery

USSOCOM / USSS

Advanced Development

Surveillance, Collection, and Operations Support

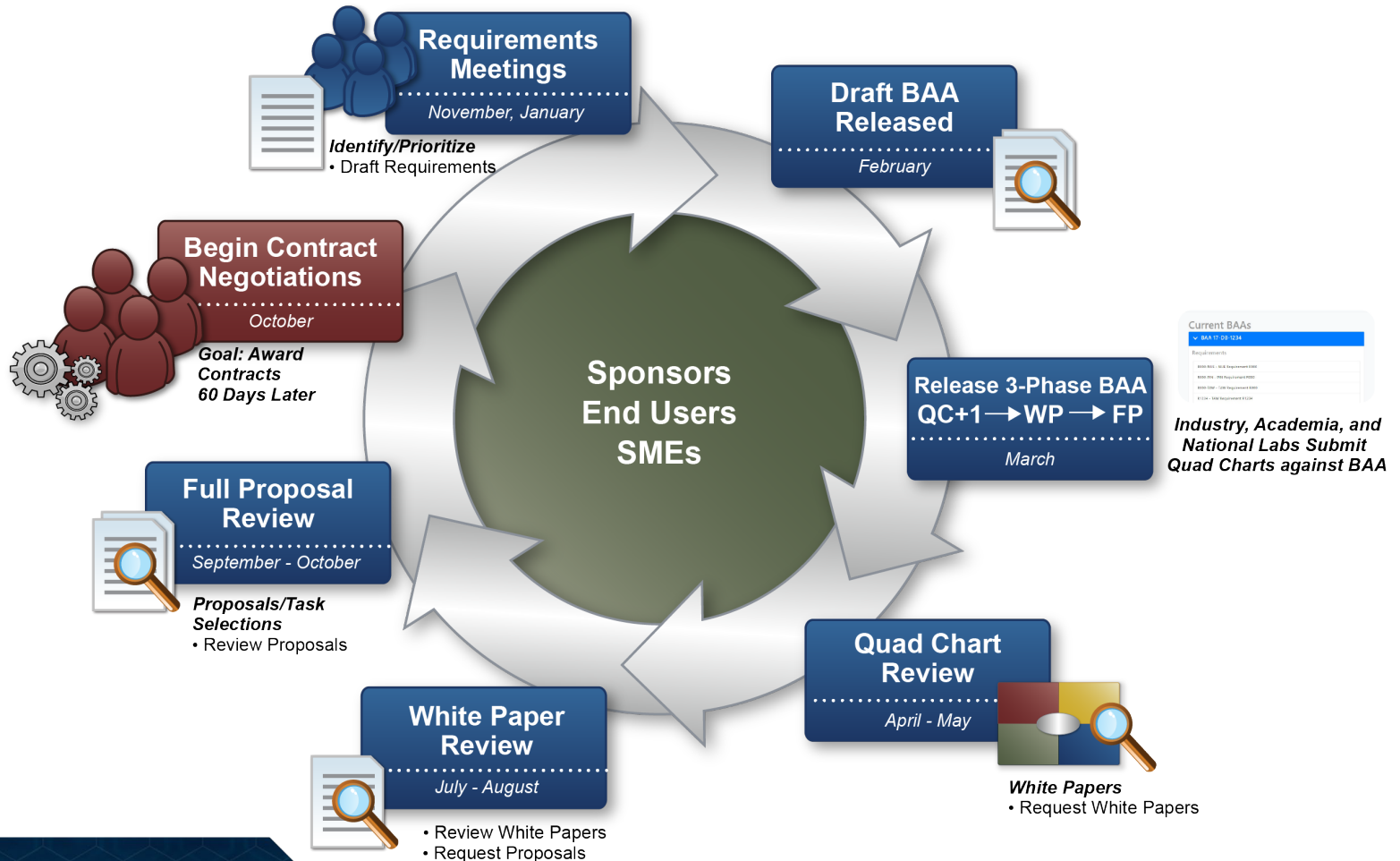
JSOC / IC

Tactical Offensive Support

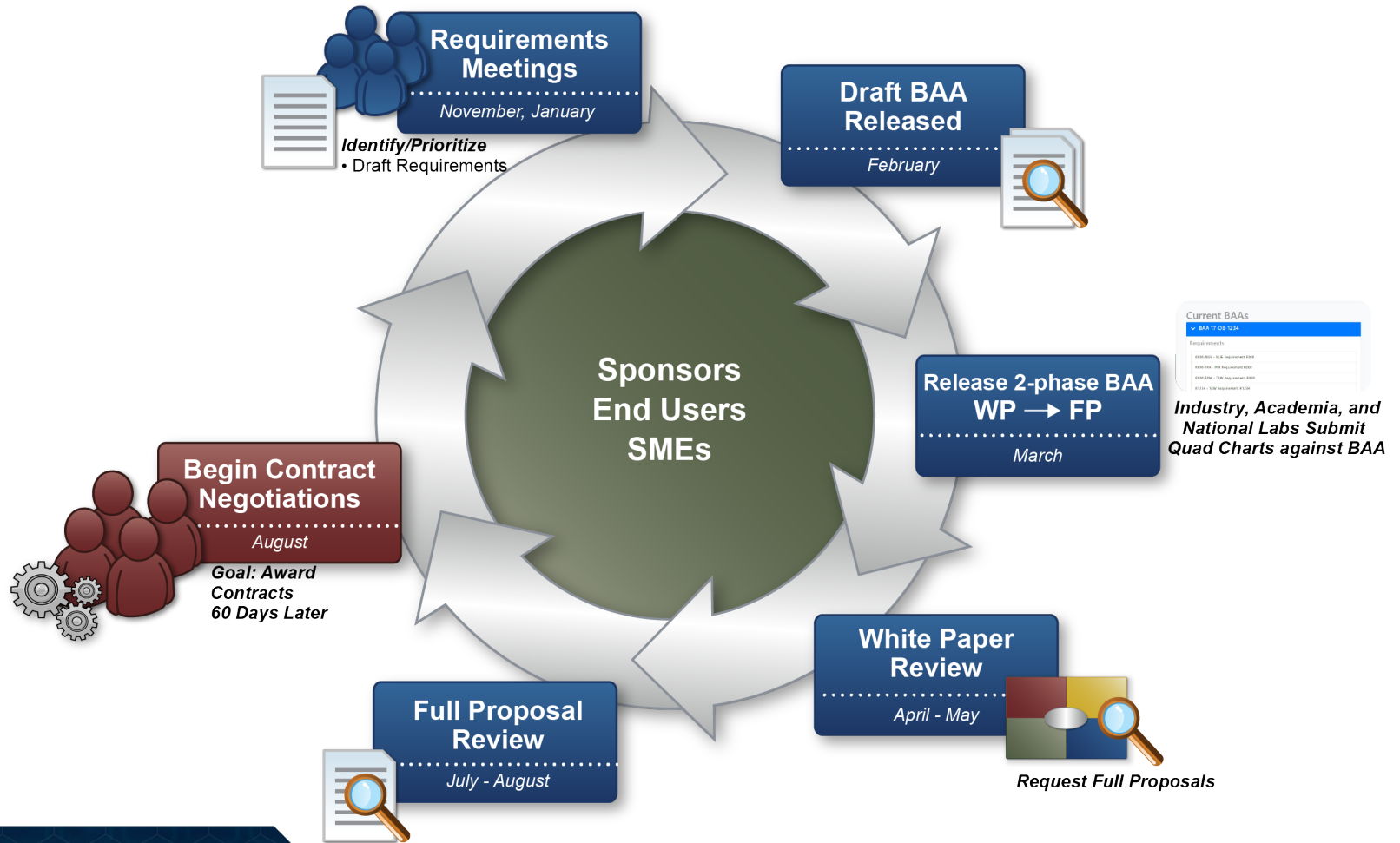
USASOC / FBI



BUSINESS CYCLE



BUSINESS CYCLE



TECHNOLOGY TRANSITION

Objective:

Affordable, operationally suitable technology in the hands of our users.

How it works:

- An integral part of IWTSD business process
 - Begins with the proposal
 - Continues throughout development
 - Requires Technology Transition Plan
- Prepares for the unexpected
- Planning assistance provided by IWTSD
- Accelerates prototype to product cycle



PARTNERSHIPS

Department of Commerce

National Institute of Standards and Technology

Department of Defense

Defense Cyber Crime Center

Defense Forensics and Biometrics Agency

Defense Intelligence Agency

- Academy for Defense Intelligence

Defense Threat Reduction Agency

National Geospatial Intelligence Agency

Office of the Under Secretary of Defense for Personnel & Readiness

- Academy for Defense Intelligence

Pentagon Force Protection Agency

Unified Combatant Commands

- U.S. Indo-Pacific Command
- U.S. Central Command
- U.S. Northern Command

U.S. Air Force

- 39th Civil Engineer Squadron
- 56th Civil Engineer Squadron
- 325th Civil Engineer Squadron
- 788th Civil Engineer Squadron
- 66th Explosive Ordnance Disposal
- 87th Explosive Ordnance Disposal
- Joint Base Andrews Air Force Base
- Air Force Installation and Mission Support Center
- Military Working Dog Program

U.S. Army

- XVIII AIRBORNE CORPS
 - 101st Airborne Division
 - 20th Engineer Brigade (A)
 - 27th Engineer Battalion (A)
 - 57th Sapper Company (A)
 - 55th Ordnance Company (EOD)
 - 65th Ordnance Company (EOD)

- 53rd Ordnance Company (EOD)
 - 911th Technical Rescue Engineer Company
 - Combat Capabilities Development Command
 - Armaments Center
 - C5ISR Center
 - Night Vision and Electronic Sensors Directorate
 - Ground Vehicle Systems Center
 - Soldier Center
 - Corps of Engineers
 - Engineering Research and Development Center
 - Geotechnical and Structures Laboratory
 - Criminal Investigation Division
 - Critical Threat Advisory Company
 - Defense Forensic Science Center
 - Questioned Documents Division
 - Joint Counter-small Unmanned Aircraft Systems Office
 - Intelligence and Security Command
 - National Ground Intelligence Center
 - Installation Management Command
 - National Guard
 - 24th Weapons of Mass Destruction Civil Support Team
 - Program Executive Office
 - Intelligence, Electronic Warfare & Sensors
 - Soldier
 - Protective Services Battalion
 - Test and Evaluation Command
 - Aberdeen Test Center
 - Training and Doctrine Command
 - Maneuver Center of Excellence
- ### U.S. Marine Corps
- 2nd Explosive Ordnance Disposal
 - G-3 Explosive Ordnance Disposal
 - Marine Corps Warfighting Laboratory/Futures Directorate
 - Deputy Commandant for Information
 - Marine Corps Information Operations Center
 - Headquarters Marine Corps
 - Deputy Commandant for Development & Integration

- Deputy Commandant for Information
 - Intelligence Division
- Deputy Commandant for Installations & Logistics
 - Marine Corps Installations Command
- Marine Corps Systems Command
 - Portfolio Manager Ground Combat Element Systems
 - Product Manager Infantry Combat Equipment
- Military Working Dog Program

U.S. Navy

- Commander, Navy Installations Command
- Explosive Ordnance Disposal Group Two
- Military Working Dog Program
- Naval Air Systems Command
 - Naval Air Warfare Center Aircraft Division
- Naval Information Warfare Systems Command
 - Naval Information Warfare Center Pacific
- Naval School Explosive Ordnance Disposal
- Naval Surface Warfare Center Indian Head Division
 - Expeditionary Exploitation Unit One
- Naval Sea Systems Command
 - Naval Undersea Warfare Center
 - Newport Division ARGUS Harbor Security
- Office of Naval Research
 - Global

U.S. Special Operations Command

- Air Force Special Operations Command
 - 492nd Special Operations Wing
 - Support Squadron (492nd SOSS)
- Army Special Operations Command
 - 1st Special Forces Group (Airborne)
 - 3rd Special Forces Group (Airborne)
 - 5th Special Forces Group (Airborne)
 - 7th Special Forces Group (Airborne)
 - C/3/7 Critical Threat Advisory Company
 - S-8 Force Modernization an Innovation Cell
- 75th Ranger Regiment
- John F. Kennedy Special Warfare Center and School
 - 2nd Special Warfare Training Group



PARTNERSHIPS

- Joint Special Operations Command
- Marine Forces Special Operations Command
 - Naval Special Warfare Command
 - Naval Special Warfare Group One
 - Naval Special Warfare Group Eight
- Special Operations Forces Acquisition, Technology, and Logistics
 - Program Executive Office-SOF Warrior
 - Program Manager Protection and Integration
 - Program Executive Office for Tactical Information Systems

Department of Energy

Department of Homeland Security

Coast Guard

Customs and Border Protection

- Commercial Targeting and Analysis Center
- Laboratories and Scientific Services

Federal Law Enforcement Training Center

Federal Protective Service

Homeland Security Investigations

- Forensic Laboratory and Document Examiners

Management Directorate

- Federal Protective Services
- Office of Biometric Identity Management
- Office of the Chief Security Officer

Science and Technology

- National Urban Security Technology Laboratory

Secret Service

- Technical Security Division

Transportation Security Administration

Department of Justice

Bureau of Alcohol, Tobacco, Firearms, and Explosives

Federal Bureau of Investigation

- Hazardous Device School
- High Value Detainee Interrogation Group

- Hostage Rescue Team

- Terrorist Explosive Device Analytical Center
- ### National Institute of Justice

Department of State

Bureau of Consular Affairs

- Office of Fraud Prevention
 - Counterfeit Deterrence Laboratory

Bureau of Diplomatic Security

- Office of Cyber and Security Technology

Department of Transportation

Office of Maritime Security

General Services Administration

Intelligence Community

Office of the Director of National Intelligence

- Central Intelligence Agency
 - High Value Detainee Interrogation Group
 - National Counterterrorism Center

Local and State Law Enforcement

Houston Police Department Bomb Squad

Massachusetts State Police Bomb Squad

Michigan Urban Search and Rescue Task Force 1

New Jersey State Police Bomb Squad

New York Police Department

- Bomb Squad

National Aeronautics and Space Administration

Australia

Department of Defence

- Science and Technology
- Special Operations Command

Canada

Canadian Security Intelligence Service

Department of National Defence

- Defence Research and Development Canada

- Ottawa Research Centre
- Suffield Research Centre
- Canadian Armed Forces
 - Army
 - 5th Canadian Division – Atlantic Canada
 - 21 Electronic Warfare Regiment
 - Canadian Joint Operations Command
 - Canadian Joint Special Operations Command
 - Canadian Special Operations Forces Command

Public Safety Canada

Royal Canadian Mounted Police

Israel

Ministry of Defense

- Israel Defense Forces
 - Ground Forces Command
 - Combat Engineering Corps
 - Yahalom Unit
- Navy

Israel National Police

Singapore

Defence Science and Technology Agency

United Kingdom

Department for Transport

Ministry of Defence

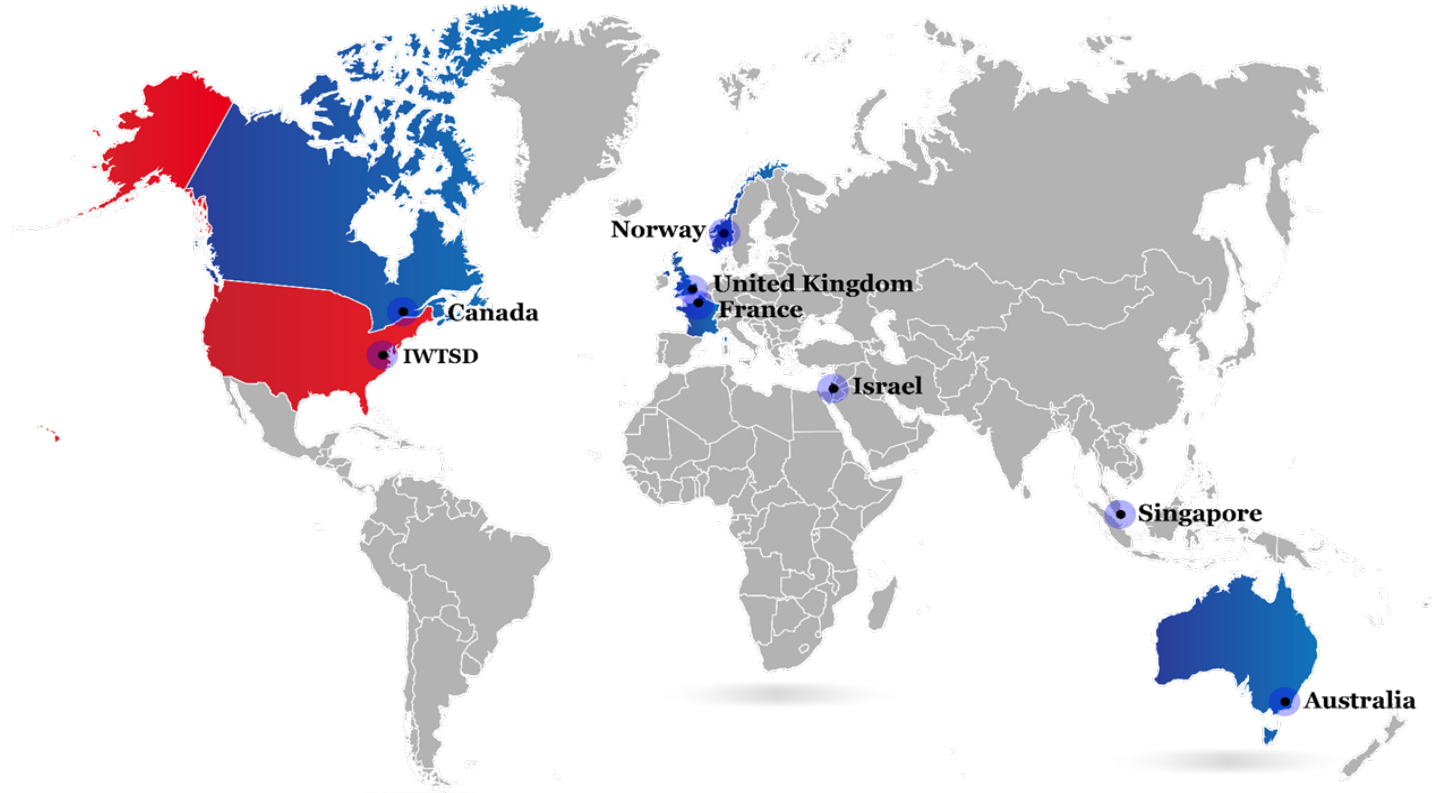
- Strategic Command
 - Special Forces
- Defence Science and Technology Laboratory
- Navy

Intelligence Community

National Protective Security Authority



INTERNATIONAL PROGRAM



Australia



Canada



France



Israel



Norway
*Currently in negotiations



Singapore



United Kingdom





IWTSD INDUSTRY DAY

Contracts/Broad Agency Announcement (BAA)

March 6, 2025

- Role of the Contracting Officer
- Historical Information
- Quad Charts
- Addendum
- Evaluation Criteria
- Lessons Learned



Roles of the Contracting Officer

- Publicizing BAA
- Overseeing Selection process
- Negotiating award and administering contracts under the BAA.



BAA STATISTICS/HISTORICAL INFORMATION

BAA #	Release Date	# of Requirements	Quad Charts Received	Awarded Amount
22S4385	23-MAR-2022	26	419	\$42,484,014
22S4387*	15-APR-2022	9	28	\$6,274,175
23S4432	27-MAR-2023	33	511	\$53,131,533
23S4431*	05-APR-2023	9	48	\$8,530,735
24S4035 (OOC)	31-JAN-2024	2	47	\$1,913,909
24S4008	29-MAR-2024	35	589	\$58,181,248

This is an approximation of the total award, including optional follow-on work.

<https://bids.iwtsd.gov/Home/DisplayAwards>

*Classified BAAs



YOUR QUAD CHART

ABC: BAA: 20-S-###
 DOC ID: SCOS-(REQUIREMENT NAME)-YOUR DOC ID



Technical Approach

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Operational Performance Capability:

- Litteris a Fabio C. Caesaris
- Consulibus redditis aegre
- ab his impetratum est summa tribunorum plebis
- Contentione ut in senatu recitarentur; ut vero ex litteris
- Ad senatum referretur, impetrari non potuit. [2] referunt consules de re publica infinite.

ROM & Schedule:

Products & Deliverables:

Corporate Information:



Addendum Content:

- Up to 1 (single sided) Pages, 8.5" x 11"
- 10pt+ font, double spaced, 1" margins
- Detail **technical data**
- Include the document identifier in header

QC-ABC-123-QC

[Please mark/classify according to the level of material contained within]

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

[1] Quo usque tandem abutere, Catilina, patientia nostra? quam diu etiam furor iste tuus nos¹ eludet? quem ad finem sese effrenata iactabit audacia? nihilne te nocturnum praesidium Palati, nihil urbis vigiliae, nihil timor populi, nihil concursus bonorum omnium, nihil hic munitissimum habendi senatus locus, nihil horum ora voltusque moverunt? patere tua consilia nonsentis, constrictam iam horum omnium scientia teneri coniurationem tuam² non vides? quid proxima, quid superiore nocte egeris, ubi fueris, quos convocaveris, quid consili ceperis quem nostrum ignorare arbitraris?

[2] O tempora, o mores! senatus haec intellegit, consul videt; hic tamen vivit. *vixit?* immo vero et iam in senatum venit, fit publici consilii particeps, notat et designat oculis ad caedem unum quemque nostrum. nos autem fortes viri satis facere rei publicae videmur, si istius furorem ac telavitamur³. ad mortem te, Catilina, duci iussu consulis iam pridem oportebat, in te conferri pestem⁴ quam tu in nos⁵ omnis iam diu⁶ machinaris.

[3] an vero vir amplissimus, P. Scipio, pontifex maximus, T. Gracchum mediocriter labefactante in statum rei publicae privatus interfecit: Catilinam⁷ orbem terrae caede atque incendiis vastare cupientem nos consules perferemus⁸? nam illa nimis antiqua praeterea, quod⁹ C. Servilius Ahala Sp. Maelium novis rebus studentem manu sua occidit, fuit, ista quondam in hac rei publicae virtus ut viri fortes acrioribus suppliciis civem perniciosum quam acerbissimum hostem coererent. habemus¹⁰ senatusconsultum in te, Catilina, vehemens et grave¹¹, non deest rei publicae consilium neque auctoritas huius ordinis: nos, nos, dico aperte, consules desumus.

¹ nos om. A et huius. Victor (Rhet. M. p. 439): post diu hab. b.

² tuam, om. CAP

³ vitamur CAP: vitamur cet.

[Please mark/classify according to the level of material contained within]



BASIC EVALUATION CRITERIA

- Basic Requirement
 - Solution must **meet** the intent of the **requirement**
- Technical Performance
 - Approach must be feasible, **achievable**, complete, and supported by a proposed technical team that has the **expertise** and **experience** to accomplish the proposed tasks



BASIC EVALUATION CRITERIA

- Cost
 - **Fair & Reasonable**
- Schedule (3 things to keep in mind)
 - Reasonable, Achievable, and Complete
- Past Performance (Phase 3 – Request for Proposal)
 - **Confidence assessment**
 - The probability of successfully performing the requirement
 - Having no relevant past performance w/ Govt will **not** be held against a vendor



LESSONS LEARNED

- Submit documents early (late is late)
- FULL disclosure of your **Data Rights**
- **Follow** the communication procedures in the **BAA**
- Use BIIDShelp@iwtsd.gov for **all correspondence**



LESSONS LEARNED

- Read and understand the BAA
- Avoid repeating the requirement
- Keep COST SAVINGS in mind
- Promote your special approach/technology





IWTSD INDUSTRY DAY

BAA Information Delivery System (BIDS)

March 6, 2025

What is BIDS?

The screenshot shows the CTTSO website interface. At the top, there are navigation links: CTTSO.GOV, SUBMITTER QUICKCARD, and RESOURCES. The main content area features a large heading 'OPEN BAAs' and a sub-heading 'BAA 19Q1007 is Open'. Below this, it states 'CTTSO is happy to announce 19Q1007 is open for submissions' and provides a link to 'Download 19Q1007 package'. To the right of the main content, there are three smaller images with red buttons: 'Register' (over a hand pointing at a glowing blue sphere), 'Login' (over a laptop screen), and 'Have a Question?' (over a blue background with question marks).

- Used to disseminate BAA related information
- Repository the BAA package
- Tracks your submissions
- Encrypts all data
- For UNCLASSIFIED submissions only!



Everyone Must Register in BIDS

CTTSO BIDS Registration Process - Please click on the appropriate button to create your registration



Invited to participate as a source selection team member to evaluate proposals?



Have an idea or product in response to a BAA requirement?



Close

- Point Chrome, Edge or Safari to <https://bids.iwtsd.gov>
- Click the “Register” button on the Homepage then click the “Create Vendor Registration” on the right



Registration Form

Username
 Enter Username

Password
 Enter Password

Re-enter password
 Re-enter Password

Contact Information

First Name
 Enter First Name

Last Name
 Enter Last Name

Street Address
 Enter Street Address

Street Address Continued

City
 Enter City

Country
 United States

State
 Select State

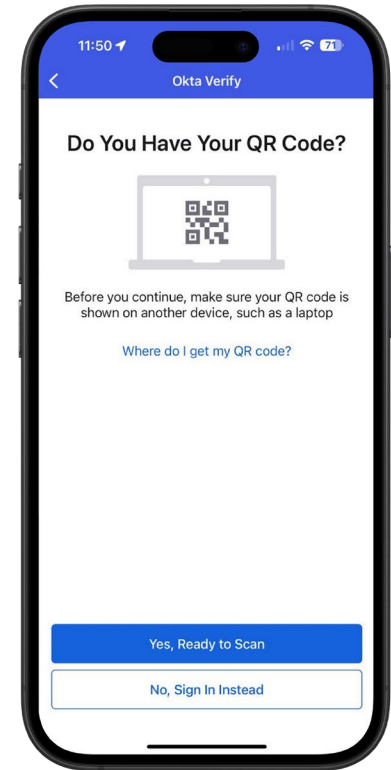
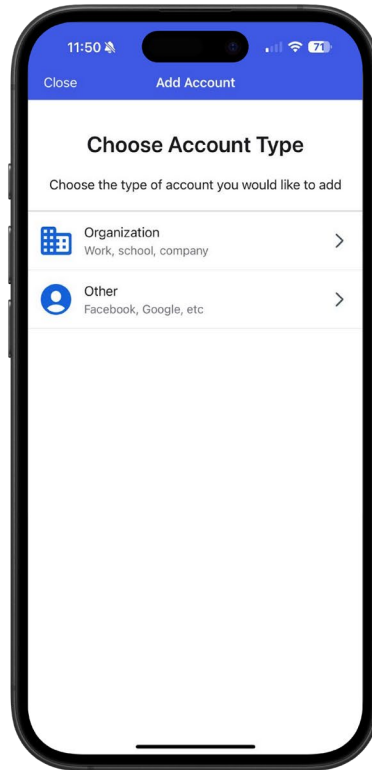
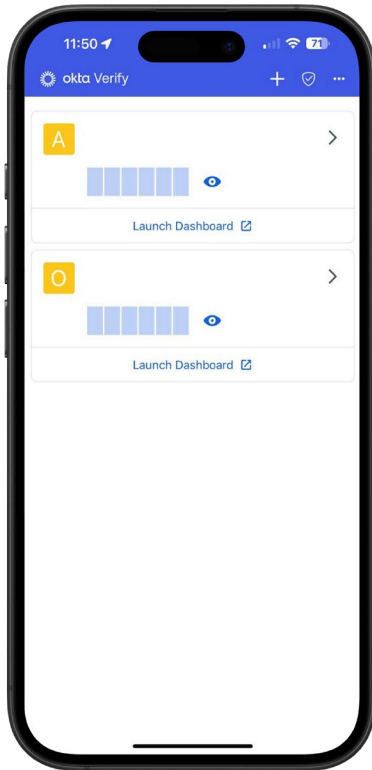
Postal Code
 Enter Postal Code

Phone Number
 Enter Phone Number (with area code)

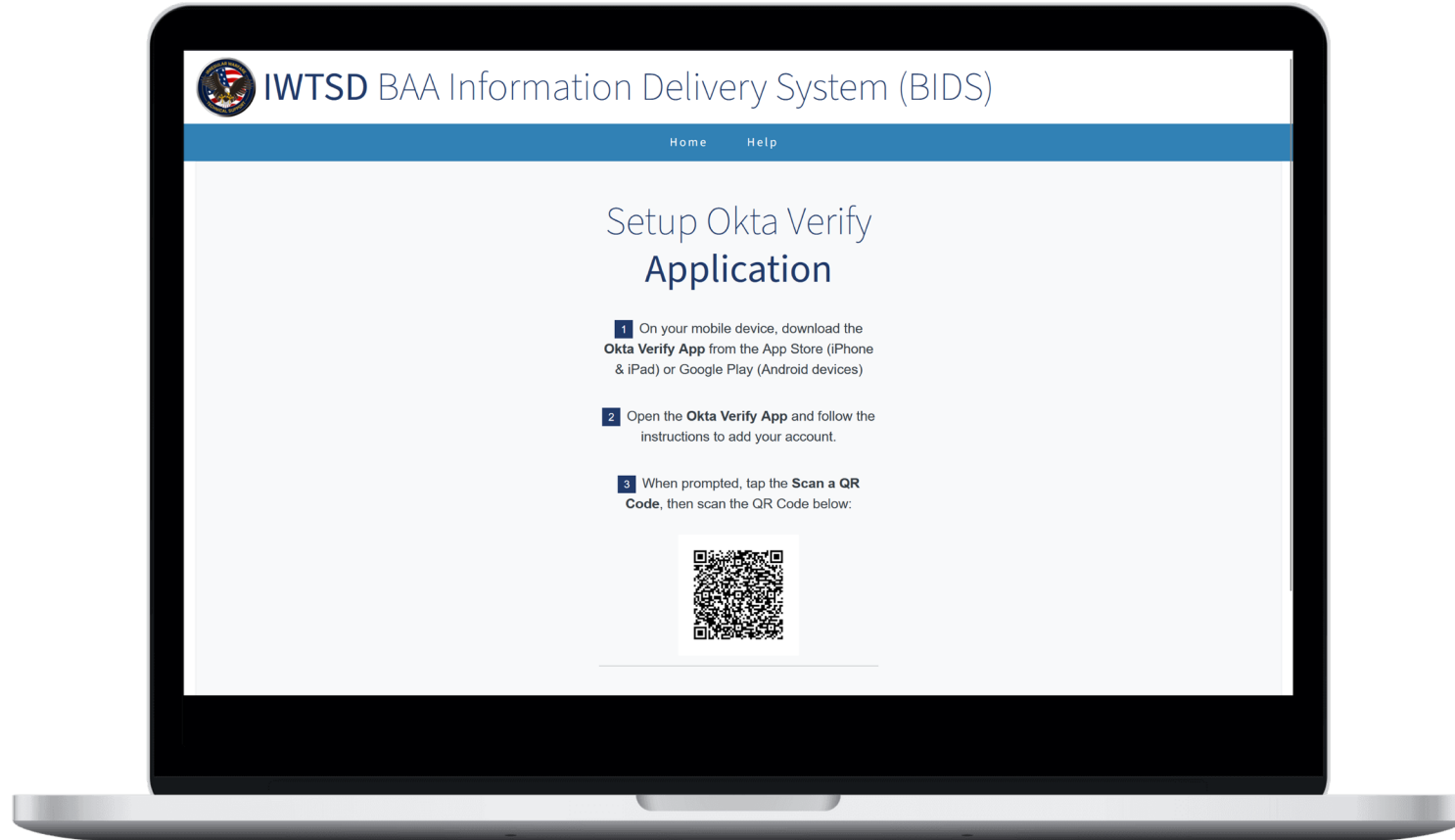
- Fill in all required fields (Marked with a red dot)
- Username appears in the Submission ID
- You may use a group email account for notifications
- All BIDS generated notification emails are sent to the address on your registration. Keep it updated!
- **NEW:** You must enroll a cell phone.

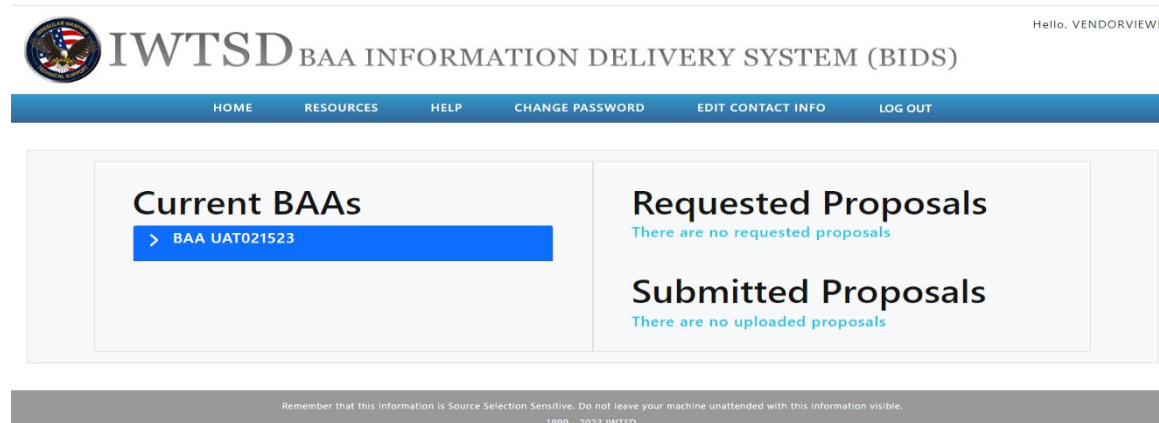


Everyone Must Register with Okta as Well



Scan QR Code After Downloading Okta





UNCLASSIFIED

UNCLASSIFIED

- Once you log in you are presented the Vendor “Dashboard”
- The “Current BAAs” shows which BAAs are open for submissions
- Click any BAA to see the requirements under it
- Click an any link to begin the submission process



Starting a Submission

Please check your proposal against the following to ensure compliance with the BAA package:

The first page of your submittal must contain:

BAA Announcement Number

Subgroup

Document Identifier

The header must contain the Document Identifier, which must be in the format described in the BAA package. Here are some examples:

ABC-R1000-VENDORUSERNAME-QC1

QRS-R8241-VENDORUSERNAME-S27A00

The last grouping of characters is the Tracking Number you will be prompted to provide when you create your proposal form.

Digital files must be submitted in the version and/or type as described in the BAA package.

Only Adobe Portable Document Format (.pdf) is allowed for Quad Chart/White Paper/Clarification file uploads.

Full Proposal file upload(s) may be submitted in Adobe Portable Document Format (.pdf), Microsoft Word (.doc/.docx), and/or Microsoft E

Graphic images must be in a format (.gif/.jpeg) that will minimize the file size and support clear display and document printing.

File sizes must be as described in the BAA package. Generally, file sizes for Quad Charts must not exceed 1 MB (1024 KB), and White Paper

Reminder: Classified proposal files will contain ONLY the Document Information, as classified material shall NOT be entered into BIDS.

See the BAA package for additional information and detailed requirements.

- Review the checklist
- We only accept submissions as a single Adobe (.pdf) file
- Click “Create Proposal” to load the submission form



Completing a Submission

● Vendor Internal Tracking Number

Enter Vendor Internal Tracking Number - 15 characters maximum.

● Proposal Title

Enter Proposal Title

● Total Cost Estimate (USD) - numbers only

0

● Estimated Project Duration in Months - numbers only

0

Want to learn about the different options you have regarding your Intellectual Property rights?

● Are you proposing unlimited rights in the technical data and/or software?

Yes, unlimited rights No, other than unlimited rights

Does your proposal require testing on humans? Do you want to know what the Government requires?

● Does the proposal include the use of human subjects in research?

Yes, human subjects will be used No, human subjects will not be used

● Upload Proposal File

Choose File No file chosen

- Review Intellectual Property Rights and Human Subject Testing statements carefully
- Titles must be unique
- Check you file size carefully
- You must upload your submission file and click the “Submit Proposal” button ***before*** the BAA closes



Checking Submission Statuses

[HOME](#)[RESOURCES](#)[HELP](#)[CHANGE PASSWORD](#)[EDIT CONTACT INFO](#)[LOG OUT](#)

Current BAAs

[> BAA UAT021523](#)

Requested Proposals

There are no requested proposals

Submitted Proposals

There are no uploaded proposals

- Do not wait for e-mails, check BIDS frequently!
- Log in and check under “Submitted Proposals” on your dashboard for the status (Accept / Reject / Under Review)
- Failure to get the automated e-mail is not grounds for an extension



The **Resources** menu item has templates for Quad charts, White papers and cover sheets. You must register to see some available materials.

Have a Question? provides access to FAQs, any responses to previously asked BAA Questions and other information.

To Request Help, click the “Have a Question” image, then scroll down and click the “Don’t see an answer to your question? Click here to create a help request” button. This sends your question to the Help Desk.

UNCLASSIFIED topics only!



Key Take-Aways

Complete your BIDS and Okta registrations at least 24 hours before BAA close

Okta (multifactor) authentication now **requires a cell phone**

All questions about Requirements must be received **within 14 days** of the BAA opening

All submission steps must be **completed** by the closing date and time to be compliant

If you have any questions, send an email to BIDSHelp@iwtsd.gov





IWTSD INDUSTRY DAY

Cybersecurity

March 6, 2025

Cybersecurity for Research and Development

- **DoDI 8500.01 – Cybersecurity:** It outlines the policies and responsibilities for protecting DoD information and IT systems.
- **DoDI 8510.01 – Risk Management Framework (RMF) for DoD Systems:** It details the processes for identifying, assessing, and mitigating risks.
- Incorporates cybersecurity **early** and **robustly** in the acquisition and system development lifecycle (**Ref. DoDI 3.a.4**):
 - Identify, mitigate, and manage unique cybersecurity risks
 - Assess and identify non-compliant controls and vulnerabilities
 - Strategically, allocate appropriate resources (people, processes, or technology) to **reduce** overall enterprise risks.



NIST 800-171 verses NIST 800-53

Feature	NIST SP 800-171 (DFARS 252.204-7012)	NIST SP 800-53
Purpose	Establishes minimum security requirements for protecting the <u>confidentiality</u> of CUI in non-federal systems.	Provides a catalog of security and privacy controls for federal information systems; addresses the <u>confidentiality, integrity, and availability</u> .
Applicability	Non-federal organizations (contractors, vendors, and suppliers) that process, store, or transmit CUI.	Federal agencies, contractors, and local governments with access to, or that operates federal information systems.
Control Families Covered	110 controls across 14 control families.	More than 900 controls across 20 control families.
Levels	Moderate baseline as standard, optional enhanced controls in NIST 800-172.	Three control baselines for low, moderate and high impact systems.
Compliance	Required for all DoD contractors that handle CUI.	Required for all DoD and Federal information systems and organizations.



Will a Project Need Cybersecurity Assessment?

If you answer **YES** to any of the following questions, then RMF applies to your effort:

- Are you **developing** DoD or Federal information systems (weapon systems, stand-alone systems, control systems, or any other type of systems with digital capabilities)?
- Will your project **transmit/process/store/display** Federal data or information (at any classification level)?
- Will your project/solution **integrate** with a DoD or other Federal information system/network?
- Will you **deploy** your product/solution on a DoD or other Federal information system/network?
- Will users **access** your product/solution remotely from a DoD or other Federal information system/network?

