DTIC Resources for Small Business

August 2016

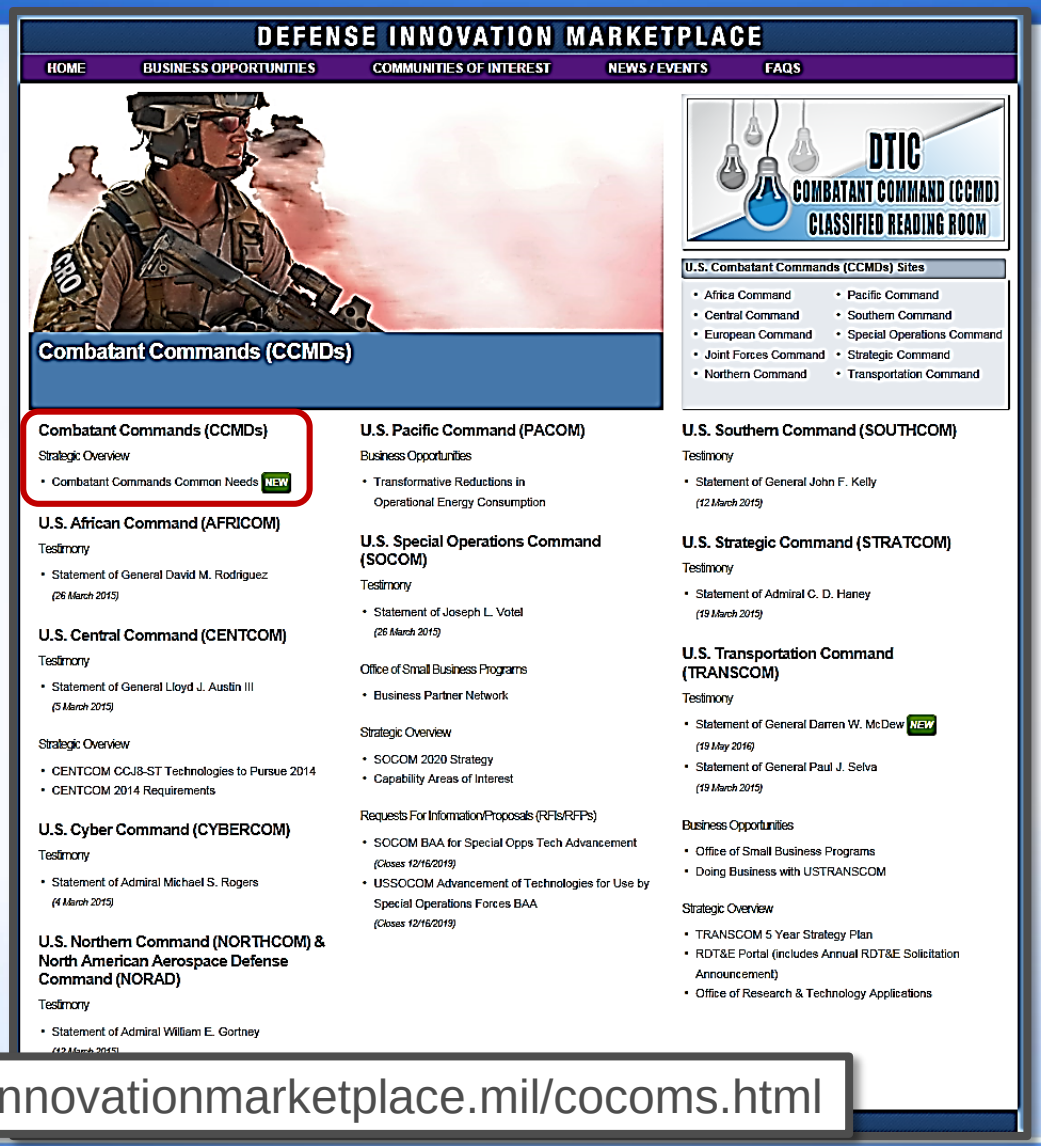
Resources:

DEFENSE INNOVATION MARKETPLACE

Combatant Command Information

http://www.defenseinnovationmarketplace.mil/

Combatant Command Needs



http://www.defenseinnovationmarketplace.mil/cocoms.html

Combatant Command Common Capability Needs

Rollup Category	Rollup Subcategory	USAFRICOM	USCENTCOM	USEUCOM	USNORTHCOM	USPACOM	USSOCOM	USSTRATCOM	USOUTHCOM	USTRANSCOM
C2/C4I/ Cyber	Architectures & Components	Communications: C4ISR for Multi-National Operations; C4ISR Data Transport; Coalition-shareable Airborne ISR Architecture	Information Sharing: Data Management–Compression and Processing Information Sharing: Multiple Domain/ Cross Domain Assurance	Improved Interoperability with Partner and Allied Capabilities	Threat Information Sharing, Collaboration, Dissemination/Mission Assurance Common Integrative Framework	Architectures and Systems to Support Information Sharing, Assured Connectivity, as well as Enhanced Interoperability among Allies and Partners	Command, Control, Communications, and Computers: Low Visibility/Low Profile/ Conformal/Multi-Spectral Antennas. Ability to selectively permit/deny net connection of personal electronic devices. Proficiency to conduct cyber-enabled SOF operations to influence foreign audiences, reduce risk to the force, and gain advantage over competitors, adversaries, and enemies.	Information Sharing: Multiple Domain/ Cross Domain Architecture	Improved interoperability with partner and Allied capabilities. Threat Information Sharing, Collaboration, Dissemination	Survivable/Secure Comms/Networks, Information Infrastructure Protection and Survivable Systems Engineering
	Cyber Defense	Communications: Cyber Freedom of Action (FOM)	Assured C2 in all environments; Ability to move and secure information across all domains ; reduced threats to automation & autonomy	Cyber COP Capable of Providing COCOM Freedom of Action	Network Resiliency	Cyber Defense/Network Security	Capabilities to counter detection in denied spaces, urban/rural areas, social media, and enhanced deception measures	Build Cyberspace Capability & Capacity	Cyber/Information Assurance. Cyber network Defense. Cyber COP capable of providing COCOM freedom of action	Cyber/Information Assurance: Defend Info and Mitigate Threats to Mobility Operations
	Sensors & Radars	ISR: Radio Frequency Direction Finding (RFDF); Stand Off Home-made/ Improvised Explosive Device (HME/IED) Detection; Fused Multi-Int'l Airborne/ FMV; Autonomy-enabled PED; Drone Sense & Avoid	Reductions in SWAP across all sensor modalities; while preserving sensor capability and sensitivity; multi-modal sensor suites which leverage onboard processing; reduction in PED for all sensors	C4: Low Vis/Low Phased Array Radio Detect and Ranging (RADAR). Optics: Undetectable	Detect, Track, and ID Air Targets/Northern Approaches Sensors	Persistent Wide Area ISR	Command, Control, Communications, and Computers: Low Vis/Low Pro Phased Array Radio Detect and Ranging (RADAR). Optics: Undetectable Aiming Laser and Advanced Sensors (persistent surveillance systems also referred to as unattended ground sensor (UGS) systems, tactical surveillance systems, and force protection systems).	Persistent Wide Area ISR/Multiple sensor integration for common integrative framework	Persistent Wide Area Surveillance to detect, track, and ID contacts of interest in CENTCOM and Caribbean approaches. UAS Due Regard Radar for Sense and Avoid foliage penetration.	Ability to Determine Security of a Landing Site for Arrival and Throughput Operations without Use of a Pre-coordinated On-site Survey as well as All-weather/Lights-out Taxi, Take-off and Landing Capability for Mobility Aircraft Operations from Prepared and Unprepared Fields.
	Communications	Communications: Centralized Commercial SATCOM Management; Language Translation; Situational Awareness; Coalition Radio Interoperability	Multi-path C2 capability in the presence of denial, spoofing & jamming; assured C2 ; improvements in underwater communications	Information Sharing/ Data Sharing with Partners and Allies.	Arctic Communication Capability: 24 Hour Persistent Comms Above 65 Degrees North	Assured, Interoperable and Cross-domain	Intelligence systems that provide unparalleled interoperability of data to support global SOF battlespace awareness for mission planning, rehearsal, analysis, & operations. Sufficiency to collect, store, retrieve, analyze, and disseminate data in near real-time (next generation Common Operating Picture)	Strategic Comms: Infrastructure Issues, and Compatibility	Information/Data sharing with partners, coalitions and allies. Assured interoperable and cross-domain comms. Caribbean Collaboration Environment	
			Assured PNT in all		Critical Time Mgmt		Position Location Information (PLI) for			

http://www.defenseinnovationmarketplace.mil/resources/CCMD_Common_Needs.pdf

Combatant Command Common Capability Needs

Rollup Category	Rollup Subcategory	USAFRICOM	USCENTCOM	USEUCOM	USNORTHCOM	USPACOM	USSOCOM	USSTRATCOM	USOUTHCOM	USTRANSCOM
C2/C4I/ Cyber	A2/AD		Ability to selectively penetrate A2AD systems at a time and location of our choosing without the need to conduct 'rollback'	ISR/Communications in a contested environment		ISR/Communications in a contested environment	SOF aviation requires precise navigation in Anti-Access/Area Denial (A2AD) environments. Navigation Independent Relative Positioning System (NIRPS) that that can provide precise navigation independent of INS and GPS. Ability to achieve denial of enemy visual augmentation systems (VAS) capability during select phases of combat operations	Cyber/ISR/Communications in a contested environment		Cyber/Information Assurance: Ability to conduct operations in a cyber contested environment.
Force Protection & Medical	Medical	Medical: Extend the "Golden Day"; Disease Surveillance and Prevention; Disease Modeling and Trauma Intervention; Remote / Austere Trauma Medicine; Medical Evacuation; Medical Informatics & Telemedicine	Medical: extend the "golden hour"; provide remote medical care in austere environments; automate medical care/monitoring during patient transport via unmanned systems	Rapid response to pandemic influenza/ infectious disease occurrence	Counter WMD preparedness and response in the domestic AOR	Counter pandemic and infectious disease	Counter WMD (CWMD) Bio-Med Systems: Tactical Portable Oxygen Generator Far-forward small team Tactical Combat Casualty Care (TCCC)-medical equipment/ protocols for rapid diagnostics, treatment, and prophylaxis. Freeze-dried Plasma/ Whole Blood Substitute	Counter WMD preparedness and response support	Biosurveillance, Countering Epidemic, Pandemic and Infectious disease. Counter IED (land, water-borne)	Virtual borders, decontamination of transportation assets, screen cargo for smuggled goods/explosives/chem-bio threats, stand-off/robotic detectors, enhance aircraft survivability
Domain Awareness	Subsurface	Maritime Domain Awareness (MDA): Beyond-Line-of-Sign; Coalition Interoperability; Automated Anomaly Detection; Common Maritime Picture	Improve all timelines associated with Mine Warfare/Q-routing; automate detection and tracking of underwater systems – manned/unmanned ; provide for assured PNT and C2 during subsurface ops – land & sea	Maritime security/ maritime domain awareness	Maritime surveillance sub-surface/ mine/under water IED	Maritime security/ maritime domain awareness		Persistent Wide Area Surveillance to detect, track, and ID air contacts of interest Workforce development	Persistent Wide Area Surveillance to detect, track, and ID air contacts of interest in CENTCOM and Caribbean Approaches. UAS Due Regard Radar for Sense and Avoid. Foliage penetration.	Capability to explore, analyze and identify trends and correlations between elements of large data sets Synchronized planning, forecasting and collaboration capabilities
Power and Energy	Power Management	Operational Energy: Expeditionary Basing & Logistics; Reduced SWaP; Alternative Energy (Solar, Wind, Geothermal); Waste-to-Energy Disposal; Expeditionary	Reduce the energy burden for forward operations; assure energy & power SCADA systems secure from attack/disruption;		Electrical energy security: ensured power where needed Electrical energy security: Secured	Secured power and energy in all mission sets. Humanitarian	Power and Energy: Undersea Manned Power System Safe, scalable non-flammable Li-Ion Cell	Secured Supervisory Control And Data Acquisition (SCADA)	Technologies that reduce dependence/consumption of fossil fuels while maintaining or improving speed, flexibility,	Technologies that reduce dependence/consumption of fossil fuels while maintaining or improving speed, flexibility, range,

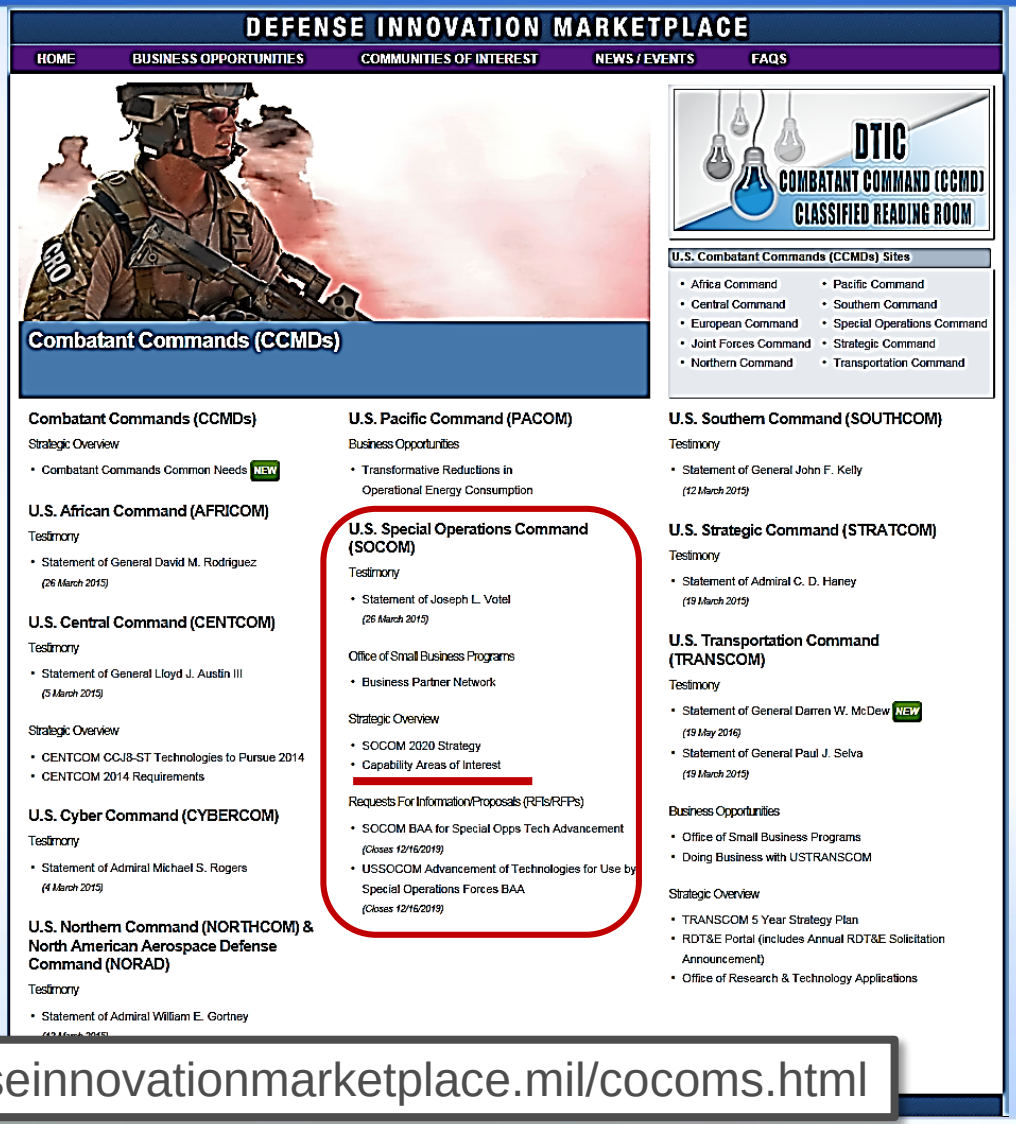
http://www.defenseinnovationmarketplace.mil/resources/CCMD_Common_Needs.pdf

Combatant Command Common Capability Needs

Rollup Category	Rollup Subcategory	USAFRICOM	USCENTCOM	USEUCOM	USNORTHCOM	USPACOM	USSOCOM	USSTRATCOM	USOUTHCOM	USTRANSCOM
Operations & Mission Support	Counter terrorism	Counter-Violent Extremist Organization (C-VEO) - Social Media Analysis; Open Source Intelligence (OSINT) Indications & Warnings. ISR: Personnel Recovery.	Create Identity Dominance across the battlespace; deny sanctuary for VEOs; leverage all forms of media to provide I&W of potential VOE action(s); improve collection, storage, transfer, and analysis of big data sets		Counter WMD preparedness and response in the domestic AOR	Counter terrorism/ extremism	Tagging, Tracking and Locating (TTL) technologies that can be used on persons and objects - technologies of interest would provide reductions in size, weight and power/price (SWaP2), improved accuracy or new capabilities	Assured PNT	Alternative platform and payload systems (APPS) for Counter-terrorism, CTOC, and CIT. Special Purpose Marine Air Ground Task Force (SPMAGTF). Counter WMD Preparedness and Response	Automated loading / offloading systems; rapid distribution technologies; innovative delivery technologies; rapidly establish ports of debarkation in austere/anti-access environments
	Counter transnational crime	Identity Activities: Biometrics, Forensics, Documentation and Media Exploitation, Denial of Anonymity, Coalition Interoperability	Assure linkages to Federal, State, Local, and International crime databases		Counter WMD preparedness and response in the domestic AOR	Counter transnational crime			Alternative platform and payload systems (APPS) for Counter-transnational organized crime	
Weapons	Non-Lethal	Non-Lethal Systems: Mobile Counter-Personnel, Counter-Materiel, Active Denial	Provide a range of non-lethal options for vessel/vehicle stop/detaining personnel, with reversibility as a key attribute		Maritime Non-Lethal Engagement/Counter UAS Non-Lethal Operations	Non-lethal capabilities across many mission sets (e.g., counter unmanned threats, Vessel/Vehicle stopping)	Scalable Effects Weapons (SEW)- counter material and counter personnel Maritime Disablement Operations (MDO)		Maritime vessel stopping Non-lethal weapons	
	Directed Energy		Provide novel and unique uses for DE: C-IED; counter-mobility; deep magazine engagements; assured C2; wireless energy transfer		Directed Energy-High power optics/laser for track/ID Directed Energy-High energy laser to engage Directed Energy-MM wave radar for Area Denial Directed Energy--High power microwave for Defense	Directed Energy: Offensive/Defensive	Airborne High Energy Laser (HEL)			
Electronic	EW management	Communications: Contested-EW	Real time characterization of the EW environment -	Capability to continue normal		Electronic Warfare and		EW management		

http://www.defenseinnovationmarketplace.mil/resources/CCMD_Common_Needs.pdf

SOCOM – Capability/Areas of Interest



http://www.defenseinnovationmarketplace.mil/cocoms.html

USSOCOM Areas of Interest

Submit

Submit Your Idea

The **Technology & Industry Liaison Office (TILO)** is the conduit to present information on capabilities to the various USSOCOM Program Executive Offices, Directorates and others responsible for the R&D, acquisition, production, and sustainment of USSOCOM material and technology platforms that support our Special Operations Forces at the headquarters. It is our duty to match your company's product/service/capability to the appropriate personnel within the command and schedule discussions or demonstrations if there is sufficient interest at the headquarters.

The process begins once your company submits a capabilities paper to USSOCOM via this website under the applicable capability area of interest. Through its Title 10 responsibilities, USSOCOM is mandated to develop, acquire, field and sustain technology in support of USSOCOM mission objectives. USSOCOM purchases those items which are deemed to be Special Operations (SO)-peculiar.

How To Begin:

USSOCOM Areas of Interest

Submit Your Idea Form

Step 1:

Review the USSOCOM areas of interest listed on this site. When you click on each category heading, you will see examples of the types of solutions we are looking for in that area.

Step 2:

Once you have completed the submission form, various subject matter experts responsible for the R&D, acquisition, production, and sustainment of USSOCOM material and technology platforms will conduct a thorough review. This review and evaluation process is usually completed in 30 days. Each idea is evaluated for its potential to meet the following criteria:

1) To be rapidly transitioned based on an immediate or imminent validated and funded need;
2) To be integrated with other technologies or programs of record; and/or
3) To be transitioned in the future or serve as a feasible solution in the requirements analysis process.

Each submission is reviewed for completeness and SO-peculiar relevance by the TILO. If more information is necessary and/or your capability is not "SO-peculiar," you will receive an email informing you to provide the required information or the capability/idea will not be evaluated as it is not appropriate for USSOCOM. The information provided through this venue may be collaborated to other technical experts and government personnel outside of the headquarters to gather additional perspectives, evaluation, or input. All information provided through this format must be UNCLASSIFIED.

Step 3:

The subject matter experts may decide that a presentation, demonstration, or other event is necessary in order to provide a comprehensive evaluation. If so, you will be contacted by the TILO to arrange the follow-on action that will be sponsored by a technical expert in the command, in accordance with FAR Part 10.001, for the purpose of market research.

A TILO briefing is an informal open dialogue between industry and the Government. The intent of these meetings is for the command to become better aware of technologies in existence or those that are close to fielding. The TILO process and briefing does not guarantee a contract or any immediate or future work with the command, but it does open the channels for idea sharing. As the mission and SOF requirements change, interest can be renewed.

All submissions will be maintained in a database/library that is available to all USSOCOM personnel for review and collaboration for 2 years and archived to an inactive database for 5 years. The information provided to USSOCOM may also be reviewed by other government agencies for the purpose of market research.

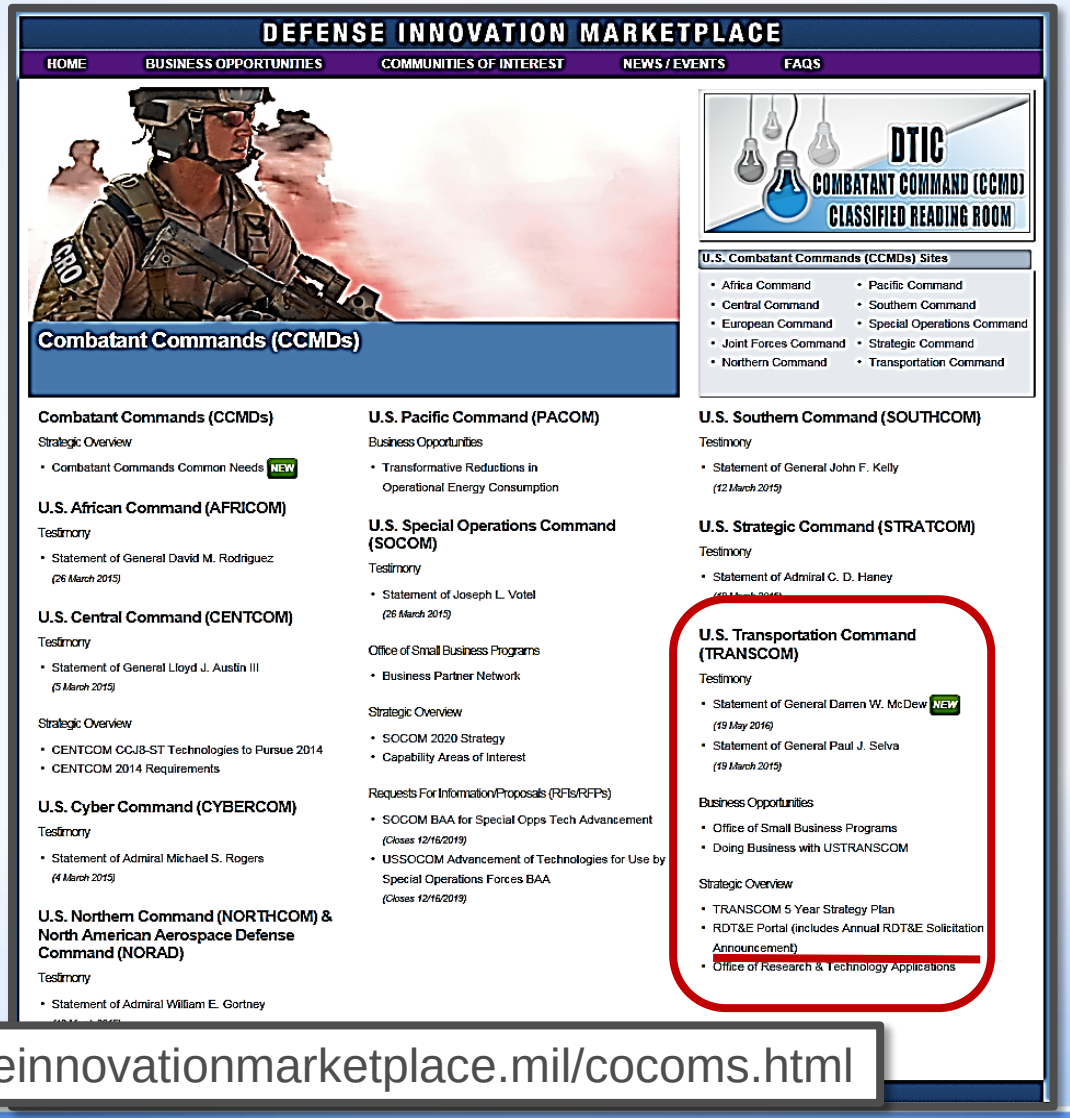
You may contact TILO at the following address:

USSOCOM
ATTN: SOF AT&/TILO
7701 Tampa Point Blvd.
MacDill AFB, FL 33621-5323

813-826-9482
813-826-9488 (fax)

TILO@socom.mil

TRANSCOM – RDT&E Portal



http://www.defenseinnovationmarketplace.mil/cocoms.html

TRANSCOM Capabilities

http://www.ustranscom.mil/cmd/associated/rdte/

TRANSCOM Capabilities

Transitioned Projects/Capabilities

- Long Range Passive RFID
- Joint Universal Causeway Interface (JUCIM)
- Predictive Analysis Capability for Optimization of Maintenance & Logistics Support
- Joint Biological Agent Decontamination System (JBADS)
- GeoSpatial Information Management/Visualization
- 2K High Altitude Low Opening Rapid Fielding
- Humanitarian Airdrop over Populated Areas
- Autonomous Mobility Applique System (AMAS)
- Autonomous Technologies for Unmanned Aerial Systems (ATUAS)
- Chemical Embrittlement Effects to Aircraft Hazard (CHEETAH)
- Collaborative Event Processing Environment (CEPE)
- Roll On/Roll Off Interface Motion Platform (RIMP)
- En-route Patient Care Module (EPCM)
- Large Vessel Interface Lift On/Lift Off (LVI Lo/Lo)
- Cross Domain Collaborative Information Environment (CDCIE)
- Hummingbird Description
- Joint Precision Airdrop System (JPADS)
- Deployable Cargo Screener (DCS)
- 463L Associate Airlift Platform (AIP)
- Opportune Landing System (OLS)
- All Mode Container Delivery System (ACDS)
- Air Mobility Ops Planning Support Tools (AMOPST)
- At Sea Selective Discharge System

http://www.ustranscom.mil/cmd/associated/rdte/?page=transitioned_projects_capabilities.cfm

TRANSCOM Capabilities

- Wireless Gate Release System (WGRS) Project Description
- Single Sign-On for Common Operating Picture (COP) Deployment
- Joint Air Logistics Information System - Next Generation (JALIS-NG)
- Analysis of Mobility Platform - Joint Integrated Campaign Model (AMP-JICM)
- End-to-End Distribution Modeling
- Total Transportation Feasibility Model (TTFM)
- Joint Modular Intermodal Distribution System (JMIDS)
- Node Management and Deployable Depot (NoMaDD)
- CONTRAIL Cargo System
- Joint Enable Theater Access Sea Ports of Debarkation (JETA-SPOD)
- Toxic Industrial Chemical (TIC) Tests
- Low Cost Low Altitude (LCLA) Airdrop
- Single Load Planning Capability (SLPC)
- Expeditionary Theater Distribution (ETD)
- Shipboard Selective Access and Retrieval System (SSARS)
- Coalition Mobility System (CMS)
- Distribution Process Nodal Model
- Fusion Center Optimization
- Common Operating Picture (COP) Deployment and Distribution (D2)
- Next Generation Wireless Communication (NGWC)
- Next Generation Logistics (NGAL)
- Data Quality (DQ) Improvement for Common Operating Picture (COP) Deployment and Distribution (D2)
- Joint Recovery and Distribution System (JRaDS)
- Cross Domain Collaborative Information Environment for Common Operating Picture (COP) Deployment and Distribution (D2)
- CERDEC Engineering for Common Operating Picture (COP) Deployment and Distribution (D2)
- Intelligent Agent for Common Operating Picture (COP) Deployment and Distribution (D2)
- Helicopter Sling Load (HSL) of Joint Precision Air Drop Systems
- Humanitarian Assistance Visibility Experiment (HAVE)
- Transportation Tracking Number (TTN)
- Cognitive Alerting and Visualization
- Automated Information System Collection & Reach-back System
- Defense Distribution Semantic Technology Investigation (D2STI)
- Semantic Ontology Effort for Common Operating Picture (COP) Deployment and Distribution (D2)
- Single Mobility System (SMS) Enterprise Web Services
- Surface Enterprise Transformation Initiative (SETI)
- Autonomous Response to Unexpected Events in DoD Terminal Operations (ARTUE–DTO)
- Container At-Sea Transfer System
- Cyber Semantic Account Management Service (C-SAMS)
- Joint Precision Air Drop System (JPADS) Next Generation Guidance, Navigation, and Control (GNC)

http://www.ustranscom.mil/cmd/associated/rdte/?page=transitioned_projects_capabilities.cfm

Resources

BUDGET TOOLS:

DOD INVESTMENT BUDGET SEARCH (R-2S AND P-40S)

DOD CONGRESSIONAL BUDGET DATA

DoD Investment Budget Search (R-2s and P-40s)

Home | 1-800-225-3842 | Email Us | About Us

DEFENSE TECHNICAL INFORMATION CENTER

Simple Search | Advanced Search | Browse Content | $ Budget Metrics | Budget Activity Definitions

DoD Investment Budget Search (R-2s and P-40s)
(formerly Research and Development Descriptive Summaries (RDDS))

- This database furnishes the Department of Defense (DOD) investment budgetary/narrative information from the President's Budget (PB) Submissions or Justification Books.
- Investment budgets include both Research, Development, Test and Evaluation (RDT&E) and Procurement.
- RDT&E programs are described on R-2s and identified by Program Elements (PE Numbers).
- Procurement programs are described on P-40s and are identified by Line Item Numbers.

Simple Search

Simple Search feature enables you to search **RDT&E** and **Procurement** collections by all of the following data elements as well as document content: ***Budget, Program Element Title, Line Item Title, Program Element Number, Line Item Number, Appropriation Number, Budget Activity, Budget Sub Activity, Fiscal Year, and Agency.***

Advanced Search

Advanced Search feature enables you to search **RDT&E** and **Procurement** collections by any of the following data elements: ***Budget, Program Element Title, Line Item Title, Program Element Number, Line Item Number, Appropriation Number, Budget Activity, Budget Sub Activity, Fiscal Year, and Agency***

Browse Content

Browse feature enables you to browse **RDT&E** and **Procurement** collections by all of the following data elements: ***Fiscal Year, Agency, Appropriation Number, and Program Element Number.***

http://www.dtic.mil/dodinvestment/#/home

Search results

0208088F

Search | Clear

Note: Since FY2011 for RDTE, and since FY2014 for Procurement, PDF documents are created from an XML file. These XML files are included as an attachment to most R-2/P-40 documents. To download the XML file: open the PDF file, find the attached file with the extension ".zzz" (paper clip icon), save this file to your local drive, change the extension from ".zzz" to ".zip", and open using WinZip.

Displaying results 1 - 10 of 16

Time: 0.076 seconds | Results: 16 | Filter: 835080 | Sort by: Select Sort Order

« ‹ 1 2 › »

Record Number: 1
Line Item Title: AFNET
Agency: Air Force
Budget Activity: 3 - Electronics and Telecommunications Equip
Line Item Number: 835080
Appropriation Number: 3080F
File Name: U_P40_835080_BSA-5_BA-3_APP-3080F_PB_2017.pdf
View PDF version | View Text version | View XML version
Snippet:

... A Program Elements for Code B Items: N/A Other Related Program Elements: **0208088F**, 0303089F, 0303112F Line Item ...

Record Number: 9
Line Item Title: AFNET
Agency: Air Force
Budget Activity: 3 - Electronics and Telecommunications Equip
Line Item Number: 835080
Appropriation Number: 3080F
File Name: P40_835080_BSA-5_BA-3_APP-3080F_PB_2016.pdf
View PDF version | View Text version | View XML version
Snippet:

... efforts. The AFNet requirement and funding for this PE in **FY17** will transition to **PE 0208088F** as the ACD weapon system. ...

.PDF Version

UNCLASSIFIED

Exhibit P-40, Budget Line Item Justification: PB 2017 Air Force | **Date:** February 2016

Appropriation / Budget Activity / Budget Sub Activity:
3080F: Other Procurement, Air Force / BA 03: Electronics and Telecommunications Equip / BSA 5: Air Force Communications

P-1 Line Item Number / Title:
835080 / AFNET

ID Code (A=Service Ready, B=Not Service Ready): A | **Program Elements for Code B Items:** N/A | **Other Related Program Elements:** 0208088F, 0303089F, 0303112F

Resource Summary	Prior Years	FY 2015	FY 2016	FY 2017 Base	FY 2017 OCO	FY 2017 Total	FY 2018	FY 2019	FY 2020	FY 2021	To Complete	Total
Procurement Quantity *(Units in Each)*	-	-	-	-	-	-	-	-	-	-	-	-
Gross/Weapon System Cost *($ in Millions)*	-	90.487	98.518	146.897	-	146.897	226.174	186.761	128.380	128.238	-	1,005.455
Less PY Advance Procurement *($ in Millions)*	-	-	-	-	-	-	-	-	-	-	-	-
Net Procurement (P-1) *($ in Millions)*	-	90.487	98.518	146.897	-	146.897	226.174	186.761	128.380	128.238	-	1,005.455
Plus CY Advance Procurement *($ in Millions)*	-	-	-	-	-	-	-	-	-	-	-	-
Total Obligation Authority *($ in Millions)*	-	**90.487**	**98.518**	**146.897**	-	**146.897**	**226.174**	**186.761**	**128.380**	**128.238**	-	**1,005.455**
(The following Resource Summary rows are for informational purposes only. The corresponding budget requests are documented elsewhere.)												
Initial Spares *($ in Millions)*	-	-	-	-	-	-	-	-	-	-	-	-
Flyaway Unit Cost *($ in Millions)*	-	-	-	-	-	-	-	-	-	-	-	-
Gross/Weapon System Unit Cost *($ in Millions)*	-	-	-	-	-	-	-	-	-	-	-	-

Description:
No efforts within this exhibit are new starts.

The AFNet exhibit includes both weapon system and non-weapon system requirements. In FY16, all AFNet weapon systems began a transition into new PEs. AFNet Weapon Systems in this exhibit are defined as follows: (1) Air Force Cyberspace Defense (ACD),(2) Cyberspace Security and Control System (CSCS), and (3) Air Force Intranet Control (AFINC). Requirements for ACD are transitioning to PE 0208088F and CSCS & AFINC are transitioning to 0303089F.

AFNet provides Commercial Off-The-Shelf (COTS) solutions to implement, deliver and upgrade installation processing nodes and boundaries, AF Gateways, enterprise network security, network situational awareness and C2 capabilities, and allows for the interface with and assured movement of information from terrestrial, air and space-based networks, thus enabling Air Force Information Operations (AFINOps). All funds used for AFNet Systems support the continued establishment and transformation of the AFINOps construct toward the standards and specifications of the DoD Joint Information Environment (JIE). The procurement efforts in this program budget line includes, but are not limited to, equipment purchase, engineering/integration, certification and accreditation, deployment, training equipment/systems, associated training and interim contractor support. Procurements implement technology and capabilities within the AFNet in accordance with the DoD IT Road map, AF Information Dominance Flight Plan, AF Cyber blueprint and the AF Network Action Plan. All activities may incorporate support to other program elements across the Air Force Information Enterprise in accordance with SAF/A6 CIO direction, the Federal Data Center Consolidation Initiative (FDCCI) and the Joint Information Environment (JIE) strategy.

PE 0207425F, AF NETWORK OPS AND COMMAND COMM

This PE was an FY16 single year PE placeholder specifically set up to execute AFNet requirements until transition to Weapon System PEs 0208088F & 0303089F in FY17.

PE 0208088F, AF DEFENSIVE CYBERSPACE OPERATIONS (ACD) WEAPON SYSTEM
This PE is not a new start. Requirements for ACD have been funded previously in 0303112F and 0207425F as part of the AFNet 835080 P-Doc. Funds may be used for other AFNet requirements if required.

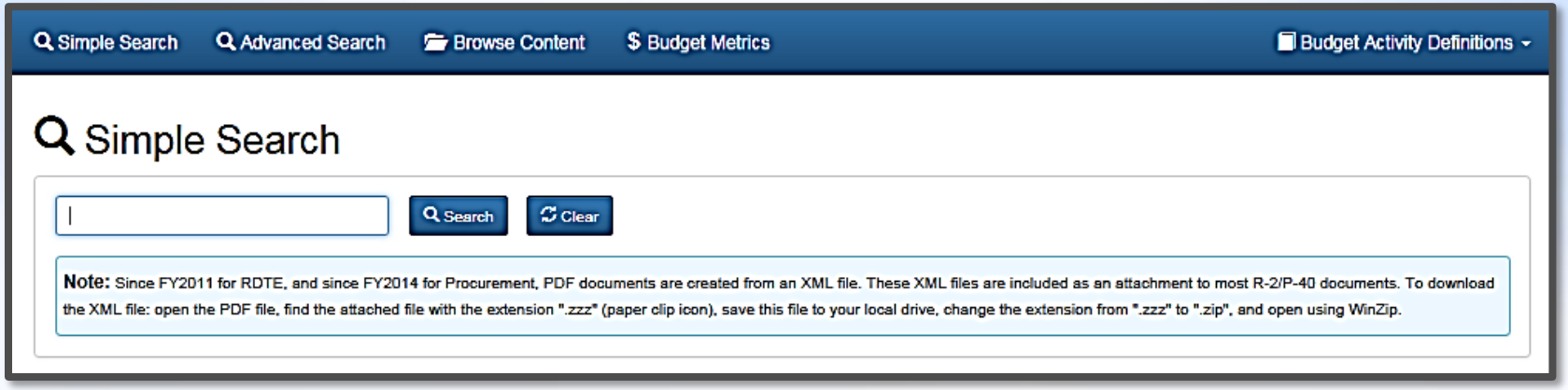
Procures and installs active defensive counter cyberspace operations and situational awareness capabilities in a Defensive Cyberspace Operations role to achieve cyberspace superiority for assigned missions. ACD procurements allow for 24/7/365 monitoring and defense of US Air Force and US Central Command, and Third Party SIPR/NIPR computer networks against hostile attacks as well as intrusion detection, network traffic analysis, network forensics analysis, countermeasure development and execution, and incident response. ACD provides indication and warning, correlation, logging, vulnerability remediation,

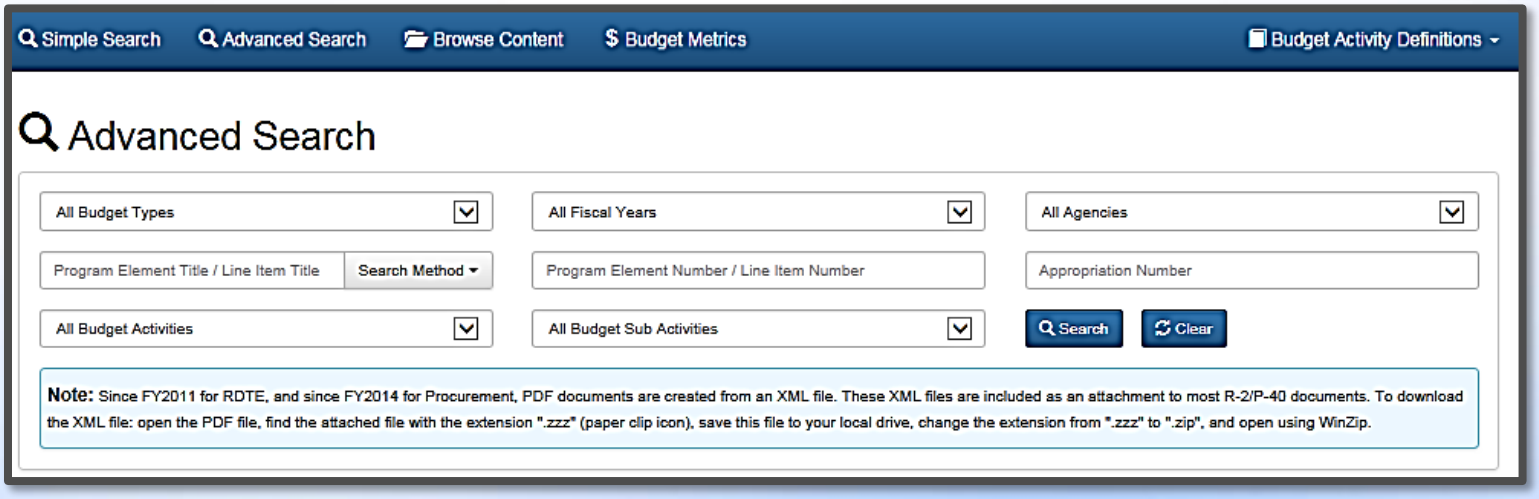
LI 835080 - AFNET
Air Force

UNCLASSIFIED
Page 1 of 17

P-1 Line #40

Simple/Advanced Search





Browse/Congressional Budget Data Collection

Simple Search | Advanced Search | Browse Content | $ Budget Metrics | Budget Activity Definitions

Browse Content

RDTE

Fiscal Year: 2000

Other Agencies: Select An Agency

PROCUREMENT

Fiscal Year: 2014

Other Agencies: Select An Agency

$ Congressional Budget Data Collection

Congressional Budget Data (CBD) Provides detailed search and analysis capabilities across the military departments and agencies for Research Development Test and Evaluation (RDT&E) data.

Start Searching »

DoD Congressional Budget Data

DoD Congressional Budget Data

Previous Reports

Welcome to the Defense Technical Information Center (DTIC) sponsored DoD Congressional Budget Data website. From this site you can access DoD Congressional Budget data, in both PDF and Excel spreadsheet formats. DTIC's goal is to post the data from each report on this site after they are filed and made available on the Congress.Gov (Library of Congress) website.

Disclaimer: *The Congressional budget data contained on this site is based on the authoritative information found on Thomas, the Library of Congress' Web site. DTIC scans the Congressional budget data and converts the information into Excel spreadsheets, which are easier to manipulate. The converted data is reviewed by DTIC to ensure accuracy; however some conversion errors can be overlooked. The scanning process is approximately 95% accurate. You can view the authoritative Congressional budget data at: https://www.congress.gov.*

Download: Select links in the table below to download PDFs or Excel spreadsheets of the associated sections of each report. Selecting the report link will allow you to download a PDF of the entire report.

FY2017 Reports	RDT&E PDF	RDT&E Spreadsheet	Procurement PDF	Procurement Spreadsheet	O&M PDF	O&M Spreadsheet	Personnel PDF	Personnel Spreadsheet
FY2017 HASC (House Report 114-537) 5MB	816K	84K	738K	164K	720K	65K	576K	36K
FY2017 SASC (Senate Report 114-255) 1.6MB	182K	71K	207K	84K	179K	46K	145K	18K
FY2017 HAC (House Report 114-577) 7.MB	1.6MB	44K	1.6MB	102K	922K	60K	557K	41K
FY2017 SAC (Senate Report 114-263) 785K	185K	42K	211K	44K	120K	31K	75K	24K
FY2017 Authorization Conference Report								
FY2017 Appropriation Conference Report								

Feedback: *If you have any questions or comments about the data on this website, or if you find any inconsistencies or errors, please send an e-mail to DOD_Congressional_Budget_help@dtic.mil.*

Detailed search and analysis capabilities across the Military Departments and Agencies for RDT&E data are available on the DoD Congressional Budget Queries website through DTIC Online (https://www.dtic.mil). The DoD Congressional Budget Queries website is normally populated with each report's RDT&E data within 48 hours of report filing.

Previous Reports

http://www.dtic.mil/congressional_budget/

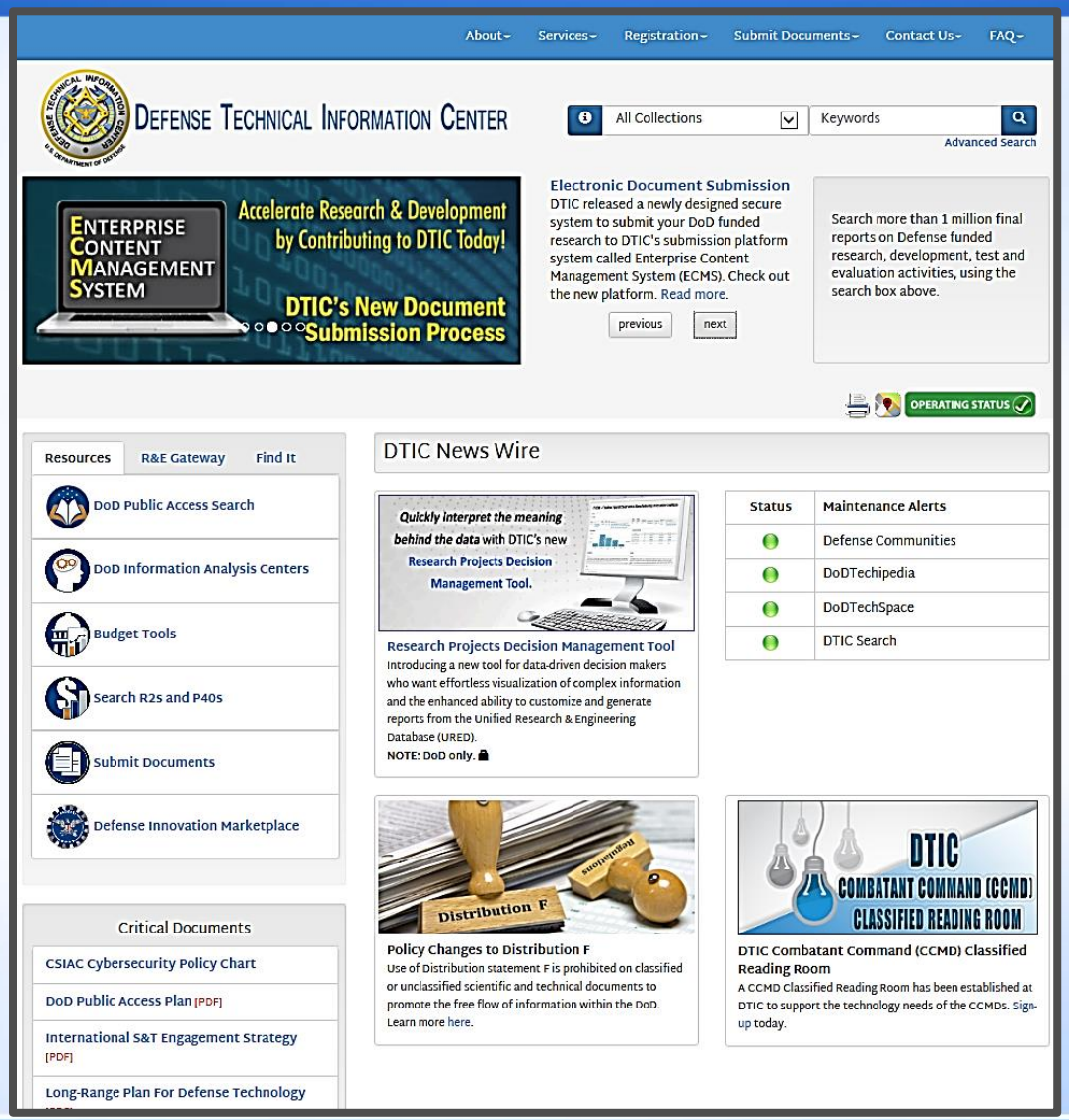
Resources

DTIC ONLINE:

PUBLICLY AVAILABLE

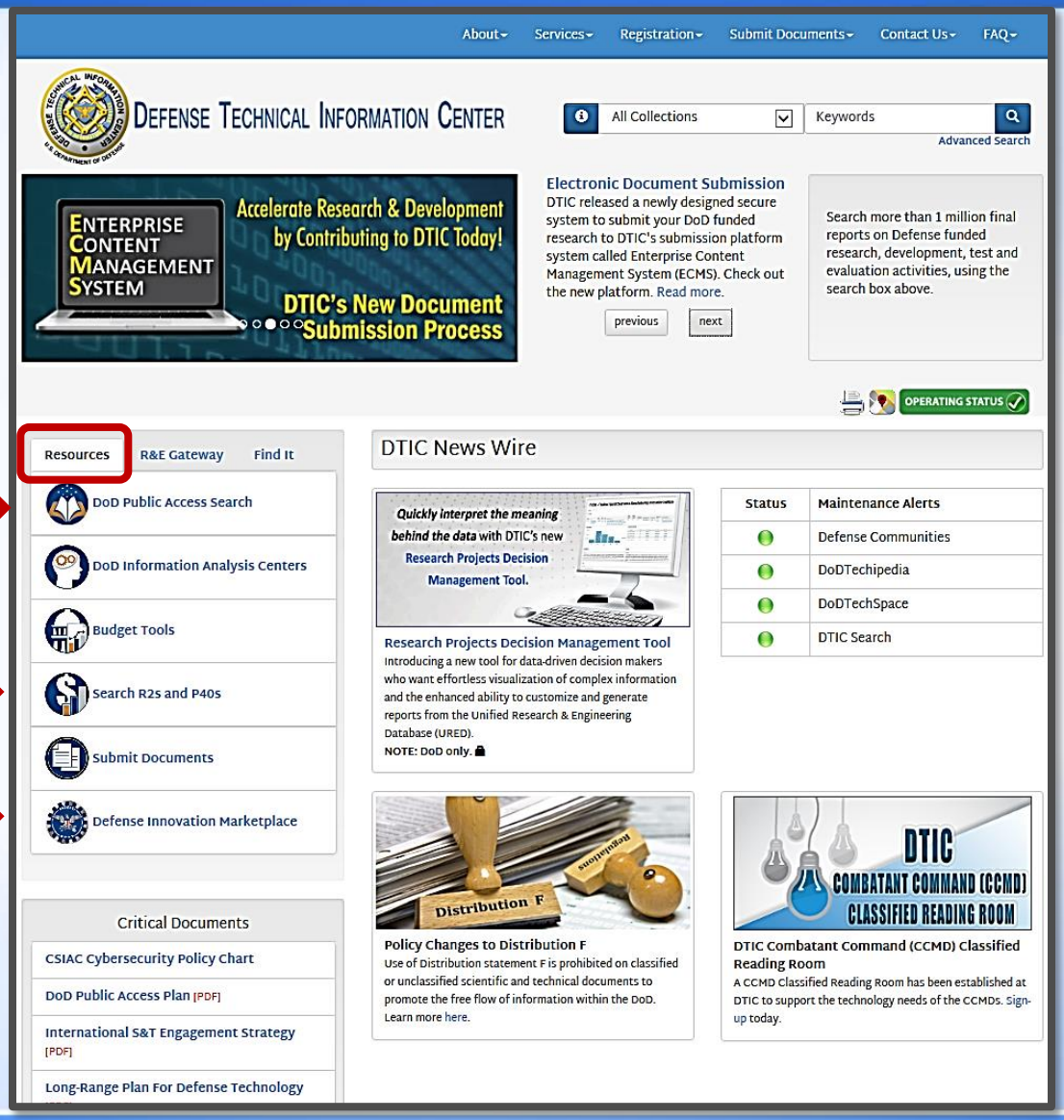
NO REGISTRATION REQUIRED

DTIC Public Site



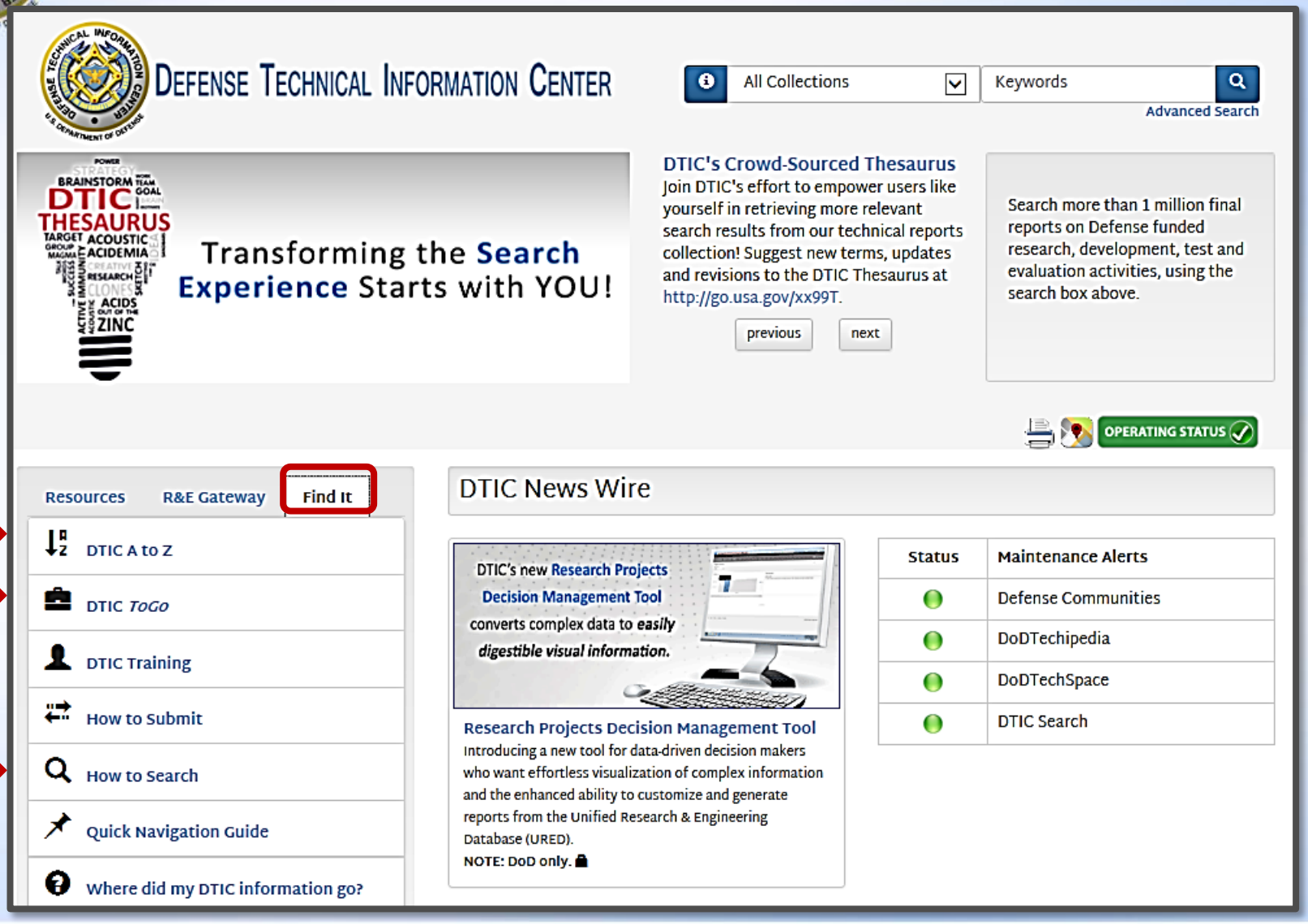
http://www.dtic.mil

Finding DTIC/DoD Resources



http://www.dtic.mil

And Another Way



Alphabetical Index

In This Section

- Acronyms
- DTIC A to Z
- FOIA
- Quick Navigation Guide
- Registration
- Research
- Submitting
- Forms

DTIC A to Z

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

About
Acronyms
ANSI/NISO Standard Z39.18-2005, Scientific and Technical Reports - Preparation, Presentation, and Preservation
ASSIST (Military Standards and Specifications)
Ask a Librarian
Air University Library Index to Military Periodicals (AULIMP)

B

Budget Tools

C

Cataloging Guidelines [PDF]
CENDI (Federal Scientific and Technical Information Managers Group)
Congressional Budget Data (DoD)
Contributing/Submitting documents to DTIC
Contributors Guidance on Submitting documents
Copyright Guidance [PDF]
Copyright Guidelines
Copyright Notice: Terms and Conditions of Use
Corporate Source Authority System Search (CSAS)
(Top of Page)

D

DDR&E & DUSD (S&T) DoD Research & Engineering Enterprise
Defense Innovation Marketplace (DIM)
Directions to DTIC Headquarters
Distribution Statements & Reasons [PDF]
Document Submission
DoD Comptroller
DoD Congressional Budget Data
DoD Directives
DoD Forms Management Program
DoD Grant Awards Website
DoD Instructions
DoD Investment Budget Search (R-2s and P-40s) (formerly Research and Development Descriptive Summaries (RDDS))
DoD Investment Budget Search Tips
DoD Issuances
DoD Lab Liaison Program
DoD Open Government
DoD Public Access

LINK: Specifications and Standards

Quick Search ASSIST

Database last updated: Aug 18, 2016

Basic Search

Enter search criteria in one or more of three text fields: Document ID, Document Number, Find Term(s). Filter search results by selecting Status or FSC/Area from drop-down lists, or by checking the box and specifying a range of document dates. Click a label for a detailed description and sample search results.

Document ID: **Document Number:** **Status:** All

Find Term1,Term2,... **For** All Terms **In** Title or Keywords or Scope

FSC/Area: Select All **Document Date:** 19-Aug-2015 **Through** 19-Aug-2016

Search Reset

http://quicksearch.dla.mil

DLA Document Services, Building 4/D, 700 Robbins Avenue, Philadelphia, PA 19111-5094.
If you have any questions, please contact the ASSIST-Help Desk team at
215-697-6396 [DSN: 442-6396].
Privacy and Security Information and Section 508 Compliance Information. Questions or comments: ASSIST Feedback.

WARNING: UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474 (THE COMPUTER FRAUD AND ABUSE ACT OF 1986) AND CAN RESULT IN ADMINISTRATIVE, DISCIPLINARY OR CRIMINAL PROCEEDINGS.

Export Controlled Access

DEFENSE LOGISTICS AGENCY
Logistics Information Services

HOME CUSTOMER SUPPORT

- JCP Home
- Search
- FAQ
- Links/Resources
- JCP Team

Joint Certification Program (JCP)
Home

United States / Canada
Joint Certification Program

The Joint Certification Office (JCO) certifies on average 4000 forms per year. However, we receive many more of which approximately 60% are returned because of inaccurate, missing or illegible information.

- In order to better serve you, our customer, please follow the guidance in the checklist. Use of it will help to ensure your submitted DD Form 2345 is correct which will allow us to process it more efficiently. Get the most current form at: DD Form 2345.

Once you complete the DD Form 2345 follow the instructions on the form to send your completed hard copy with supporting documentation, if applicable, to the following address by postal service or courier:

U.S./Canada Joint Certification Office
DLA Logistics Information Services
Hart, Dole, Inouye Federal Center
74 Washington Ave., North
Battle Creek, MI. USA 49037-3084

https://www.dlis.dla.mil/jcp

Overall, your company's certification will process faster by initially providing the correct information and ensuring it matches your Cage Code or NATO Cage Code information in BINCS. We are pleased to advise the JCO has taken steps to improve the time it takes to process the DD Form 2345 by adding staff, improving processes, and identifying technology improvements for our database.

Once the JCO receives the application from a company it is logged into a tracking database and assigned a tracking number; it is then sent to research for verification. If during the research process the information is correct it gets sent to processing for certification. If there are errors, then the form is returned to the customer with an explanation of what is wrong and instructions on what needs to be done to correct it.

During the actual certification process the JCP certification number gets assigned and the database information is updated to reflect current information. The form is stamped as certified and emailed back to the Data Custodian listed on the form using the email address on the form. The JCP website provides a search function to see if a company is certified and when it expires.

Common Errors in DD Form 2345 Submissions Occur in the following areas:

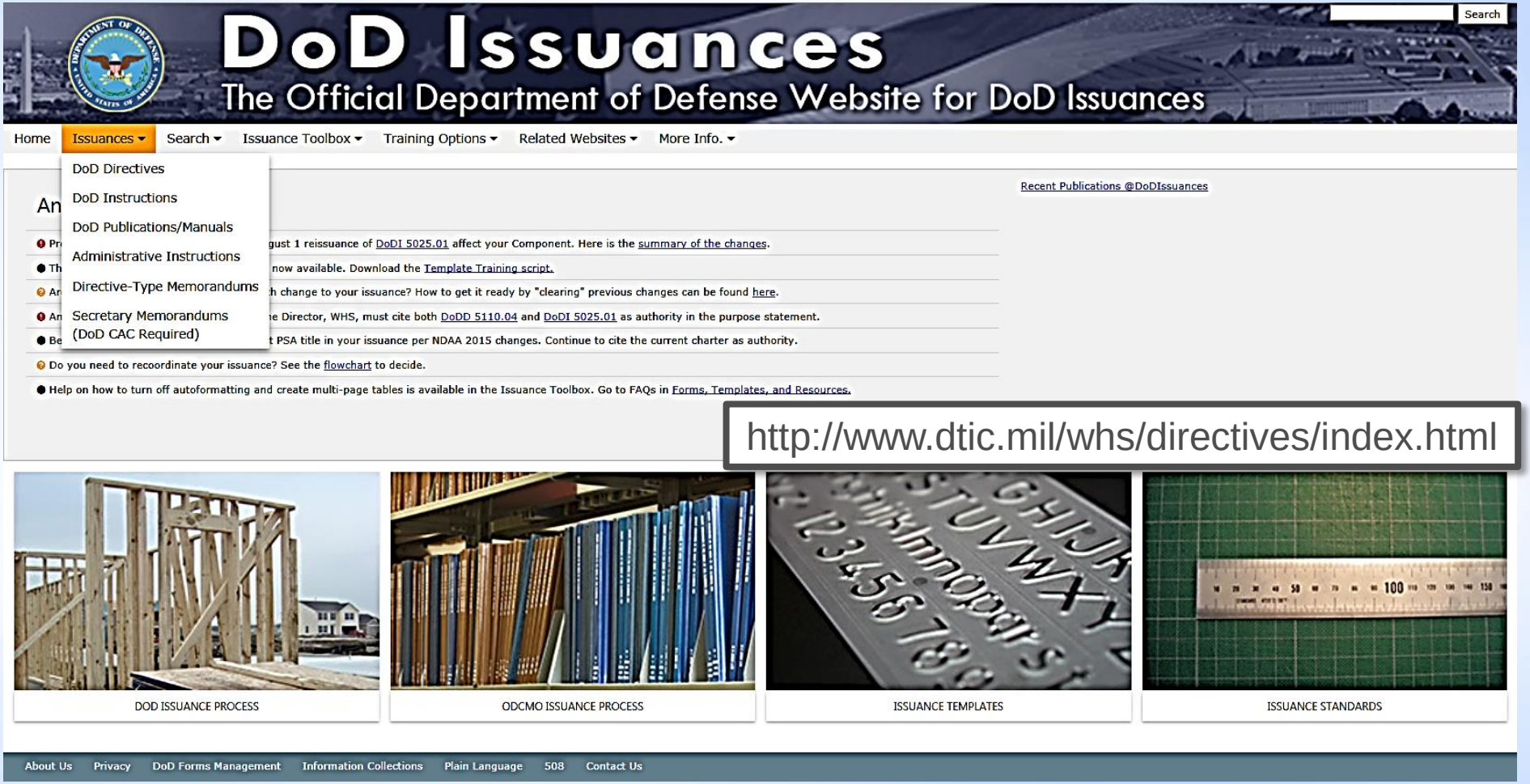
LEGAL NAME: the Block 2 information on the form must exactly match your company's legal name and address for your Cage Code or NATO Cage Code in BINCS. No nicknames, acronyms or abbreviations unless they are in your legal name.

Cage Code or NATO Cage Code: failure to obtain a Cage Code or NATO cage Code or to provide it on the form in Block 2D for the location being certified.

Incorrect Physical Address: the address used in Block 2B must be the physical location of the site being certified. Not the mailing address unless it's the same. Not the headquarters but the location being certified.

Data Custodian's Location: this person must be employed at the location being certified. There can be only one Data Custodian per location unless the location has multiple CAGE codes then each CAGE needs its own different custodian if being certified. (Let's talk about past policy)
Business Description: a proper business description must be included in Block 4. It should describe the nature of your business not why you need the certification.

LINK: DoD Directives, Instructions, & More



http://www.dtic.mil/whs/directives/index.html

NDIA Conference Proceedings @ DTIC

http://www.dtic.mil/ndia

Conference Proceedings

2016 2015 2014 2013 2012 2011 2010 2009 2008 2007

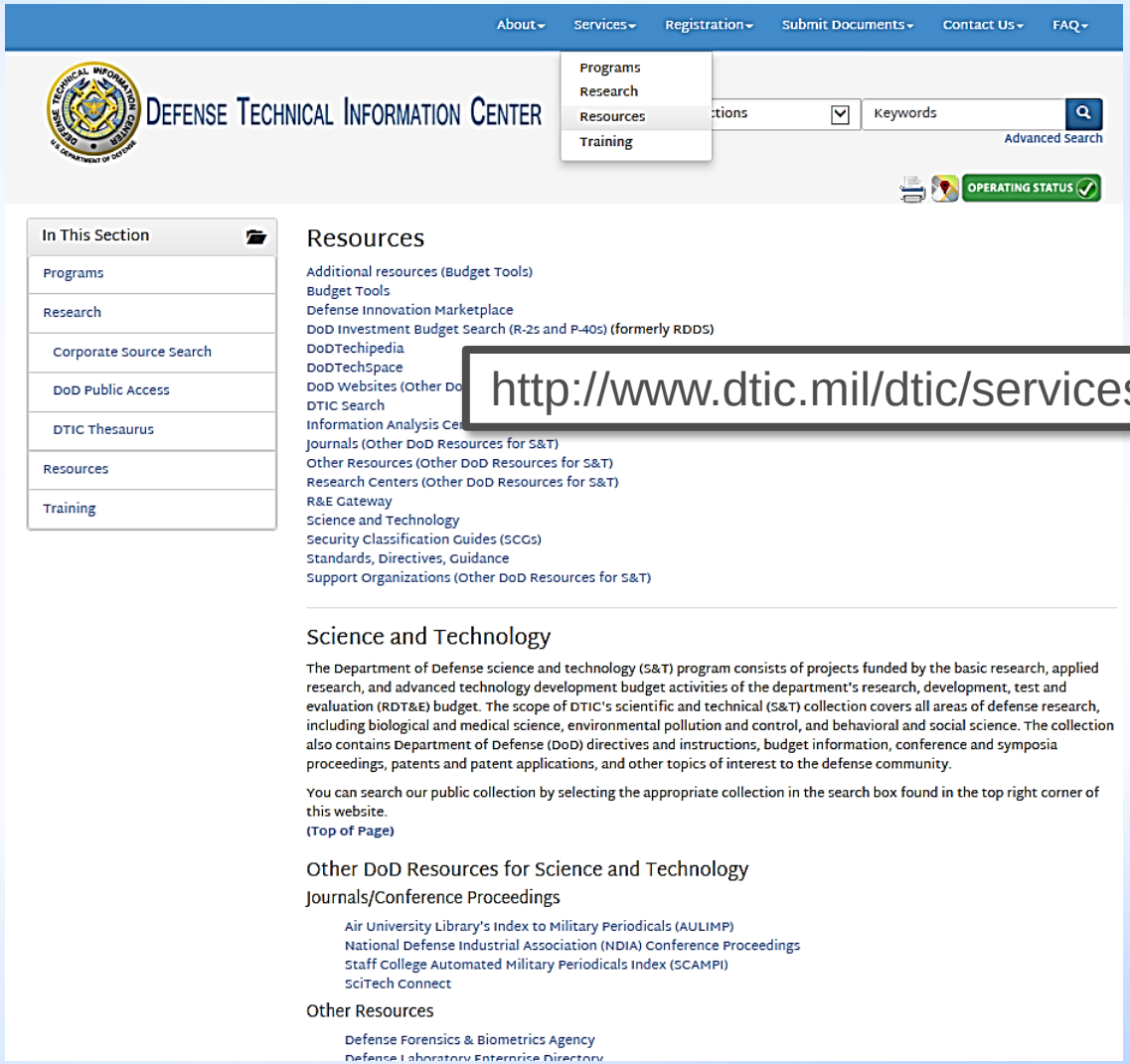
2016

- U.S.-Japan Defense Industry Conference, 3 May 2016, Arlington, VA
- 32nd Annual National Logistics Forum, 18 - 20 April 2016, Washington, DC
- 2016 Armament Systems Forum, 25 - 28 April 2016, Fredericksburg, VA
- Medical Research, Development and Acquisition in Support of the Warfighter, 19 - 20 April 2016, Ellicott City, MD
- 17th Annual Science & Engineering Technology Conference, 12 - 14 April 2016, Tampa, FL
- 2016 Munitions Executive Summit , 29 - 31 March 2016, Parsippany, NJ
- Precision Strike Annual Review (PSAR-16), 15-16 March 2016, Springfield, Va
- Ground Robotics Capabilities Conference & Exhibition, 2-3 March 2016, Springfield, VA
- 31st Annual National Test and Evaluation Conference, 2-3 March 2016, McClean, VA
- 2016 Human Systems Conference, 9-10 February 2016, Springfield, Va
- 27th Annual SO/LIC Symposium & Exhibition, 19-21 January 2016, Washington, DC
- NDIA TRI-Association Small Business Advisory Panel (TRIAD) Conference, 11 February 2016, Orlando, FL

2015

- 2015 Global Demilitarization Symposium, 7-9 December 2015, Parsippany, NJ
- 20th Annual Expeditionary Warfare Conference, 27-29 October 2015, Norfolk, VA
- 25th Annual Precision Strike Technology Symposium (PSTS-15), 27-29 October 2015, Laurel, MD
- 18th Annual Systems Engineering Conference, 26-29 October 2015, Springfield, VA
- 12th National Small Business Conference, 24 September 2015, Springfield, VA
- 2015 TRIAD Small Business Advisory Panel, 23 September 2015, Springfield, VA
- UK-Canada-Australia-US Quadrilateral Conference, 14 September 2015, Ottawa, Canada
- 2015 Joint Service Power Expo, 24 - 27 August 2015, Cincinnati, OH
- 2015 Tactical Wheeled Vehicle Conference, 24 - 26 August 2015, Reston, VA
- Global Explosive Ordnance Disposal (EOD) Symposium & Exhibition, 27 - 28 July 2015, Bethesda, MD
- NDIA Annual CBRN Defense Conference and Exhibition, 21 - 23 July 2015, Edgewood, MD
- 6th Annual Integrated Air and Missile Defense Symposium, 25 June 2015, Laurel, MD

Services



http://www.dtic.mil/dtic/services/resources.html

DoD Grants Database

Home | Contact | Help | Log In

DoD Grant Awards

https://dodgrantawards.dtic.mil/grants/#/home

Simple Search | Advanced Search

Welcome

Welcome to the Department of Defense (DoD) Grant Awards Website. This website was established in response to a statutory requirement contained in Section 8123 of the fiscal year 2015 DoD Appropriations Act (Division C of the Consolidated and Further Continuing Appropriations Act, Public Law 113-235). This website contains publicly-searchable descriptive abstracts of DoD grant awards from December 9, 2014 (the date of passage of the Act), along with other grant award information. Members of the public may conduct searches using a variety of fields and/or keywords, and view or download the results. For more information on the DoD grant award data available from this website, please see the frequently asked questions (FAQ) section under the Help menu.

Notice

DoD awarding offices are in the process of uploading DoD grant awards dating from December 9, 2014 to the website. If you are looking for a particular grant award from that date and it does not appear in your search, please try again at a later date. We will post a message here when all FY 2015 awards have been entered. DoD grant award information for fiscal years after 2015 will be entered on a continuing basis as grant awards are made.

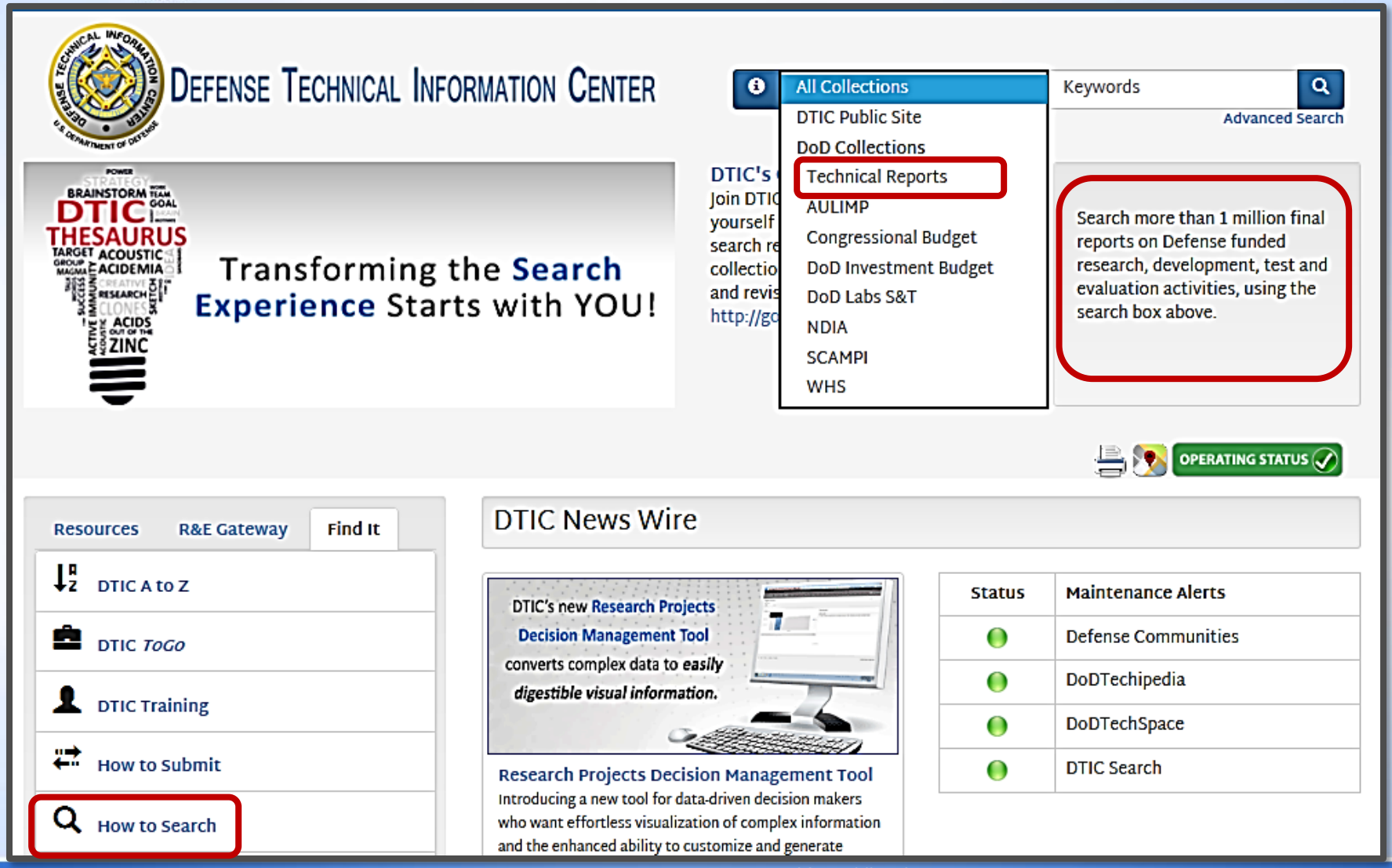
Simple Search

Search by the following fields: ***project title, award abstract, award number, DoD awarding office, and recipient organization name.***

Advanced Search

Search by these additional fields: **award amount, fiscal year, funding agency, start/end dates, creation/modified dates, and POC name.**

Search: Mining DTIC Resources



Search Results: Technical Reports

Search

Results **1** - **10** of about **6630** for **cyber**. Search took **0.12** seconds.

Next >

Sort by date / Sort by relevance

Related search keywords

- cyber operations
- cyber warfare
- cyber domain
- cyber attacks
- cyber physical systems
- cyber security
- cyber defense
- cyber force
- cyber intelligence
- cyber terrorism

1. Closing the **Cyber** Gap: Integrating Cross-Government **Cyber** Capabilities to Support the DHS **Cyber** Security Mission
   ... Title : Closing the **Cyber** Gap: Integrating Cross-Government **Cyber** Capabilities to Support the DHS **Cyber** Security Mission. ...
   www.dtic.mil/docs/citations/ADA620564 - 31k - 2014-12-01 - Cached - PDF

2. For the Common Defense of Cyberspa[illegible]plications of a US **Cyber** [illegible]a on Department of Defense **Cyber** Operations
   ... Title : For the Common Defense of Cy[illegible]pace: Implications of a U[illegible]ber Militia on Department of Defense **Cyber** [illegible]ations. ...
   www.dtic.mil/docs/citations/ADA623946 - 2[illegible] 2015-06-12 - Cache[illegible]DF

3. **Cyber**-Argus: Modeling C2 Impacts of **Cyber** Atta[illegible]
   ... Title : **Cyber**-Argus: Modeling C2 Impacts of **Cyber** Attacks. ... Abstract : **Cyber** security is often only seen as protecting networks. ...
   www.dtic.mil/docs/citations/ADA607024 - 30k - 2014-06-01 - Cached - PDF

4. **Cyber** Insurance - Managing **Cyber** Risk
   ... Close. Accession Number : ADA623798. Title : **Cyber** Insurance - Managing **Cyber** Risk. Descriptive Note : Final rept. Corporate ...
   www.dtic.mil/docs/citations/ADA623798 - 28k - 2015-04-01 - Cached - PDF

5. Attribution, Delayed Attribution and Covert **Cyber**-Attack: Under what Conditions should the United States Publicly Acknowledge Responsibility for **Cyber** Operations?
   ... Title : Attribution, Delayed Attribution and Covert **Cyber**-Attack: Under what Conditions should the United States Publicly Acknowledge ...
   www.dtic.mil/docs/citations/ADA607746 - 28k - 2014-03-01 - Cached - PDF

6. Unconventional **Cyber** Warfare: **Cyber** Opportunities in Unconventional Warfare
   ... Close. Accession Number : ADA607604. Title : Unconventional **Cyber** Warfare: **Cyber** Opportunities in Unconventional Warfare. ...
   www.dtic.mil/docs/citations/ADA607604 - 29k - 2014-06-01 - Cached - PDF

7. Offense-Defense Theory Analysis of Russian **Cyber** Capability
   ... Close. Accession Number : ADA620663. Title : Offense-Defense Theory Analysis of Russian **Cyber** Capability. Descriptive Note : Master's thesis. ...
   www.dtic.mil/docs/citations/ADA620663 - 30k - 2015-03-01 - Cached - PDF

8. Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the **Cyber** Domain
   ... Close. Accession Number : ADA617164. Title : Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the **Cyber** Domain. ...
   www.dtic.mil/docs/citations/ADA617164 - 29k - 2013-01-01 - Cached - PDF

OR

1. [PDF] Red Sea Outflow Experiment (REDSOX): DLD2 RAFOS Float Data Report February 2001 - March 2003
   ... 159 N **010308 010308** 12.218 47.998 020308 11.844 45.666 00 r160 N 010305 **010308** 13.502 48.004 020304 13.025 49.810 00 ...
   www.dtic.mil/dtic/tr/fulltext/u2/a432810.pdf - 858k - 2005-01-01 - Text Versio[illegible] - **Citation**

Database Entry

DEFENSE TECHNICAL INFORMATION CENTER

Select Search | Keywords

Accession Number : ADA620564

Title : Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to Support the DHS Cyber Security Mission

Descriptive Note : Master's thesis

Corporate Author : NAVAL POSTGRADUATE SCHOOL MONTEREY CA

Personal Author(s) : Lowery, Edward W

Full Text : http://www.dtic.mil/get-tr-doc/pdf?AD=ADA620564

Report Date : Dec 2014

Pagination or Media Count : 139

Abstract : Following the 9/11 terror attacks, the Department of Homeland Security (DHS) was mandated to ensure the security of the nation's cyber-supported critical infrastructure, which is predominantly privately owned and outside of the control of the U.S. government. This thesis examines the development of the government's cyber-security policies and primary operational entities through their lawful authorities and capabilities. The thesis also examines and contrasts the effectiveness of DHS's technology-centric, cyber-security approach, the deterrent effect realized through law enforcement cyber operations, and the suitability and effectiveness of the utilization of military or intelligence agencies, specifically the FBI, National Security Agency or Department of Defense, to fulfill the nation's domestic cyber-security mission. Evidence suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information-sharing programs, and develop cyber incidence response teams while not fully utilizing the U.S. Secret Service's legal authorities and capabilities in furtherance of the department's mission. Recommendations are offered to develop a whole-of-government cyber-security policy for an effective, integrated, cyber-security operation through the utilization of agency-specific authorities and capabilities, while protecting our nation's critical infrastructure and our citizens civil liberties.

Descriptors : *COMPUTER NETWORK SECURITY, *HOMELAND SECURITY, CIVIL AFFAIRS, COLLABORATIVE TECHNIQUES, DEFENSE SYSTEMS, DETERRENCE, ESPIONAGE, FEDERAL BUDGETS, HACKING(COMPUTER SECURITY), INFORMATION ASSURANCE, INFORMATION SYSTEMS, INTELLIGENCE, INTERNET, INTRUSION DETECTION(COMPUTERS), NATIONAL SECURITY, NETWORK ARCHITECTURE, POLICIES, TEAMS(PERSONNEL), TERRORISTS, THESES, VULNERABILITY

Subject Categories : Government and Political Science
Sociology and Law
Computer Systems Management and Standards

Distribution Statement : APPROVED FOR PUBLIC RELEASE

Accession Document Number: Key to DTIC Records

DEFENSE TECHNICAL INFORMATION CENTER

Select Search | Keywords

Accession Number : ADA620564

Title : Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to Support the DHS Cyber Security Mission

Descriptive Note : Master's thesis

Corporate Author : NAVAL POSTGRADUATE SCHOOL MONTEREY CA

Personal Author(s) : Lowery, Edward W

Full Text : http://www.dtic.mil/get-tr-doc/pdf?AD=ADA620564

Report Date : Dec 2014

Pagination or Media Count : 139

Abstract : Following the 9/11 terror attacks, the Department of Homeland Security (DHS) was mandated to ensure the security of the nation's cyber-supported critical infrastructure, which is predominantly privately owned and outside of the control of the U.S. government. This thesis examines the development of the government's cyber-security policies and primary operational entities through their lawful authorities and capabilities. The thesis also examines and contrasts the effectiveness of DHS's technology-centric, cyber-security approach, the deterrent effect realized through law enforcement cyber operations, and the suitability and effectiveness of the utilization of military or intelligence agencies, specifically the FBI, National Security Agency or Department of Defense, to fulfill the nation's domestic cyber-security mission. Evidence suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information-sharing programs, and develop cyber incidence response teams while not fully utilizing the U.S. Secret Service's legal authorities and capabilities in furtherance of the department's mission. Recommendations are offered to develop a whole-of-government cyber-security policy for an effective, integrated, cyber-security operation through the utilization of agency-specific authorities and capabilities, while protecting our nation's critical infrastructure and our citizens civil liberties.

Descriptors : *COMPUTER NETWORK SECURITY, *HOMELAND SECURITY, CIVIL AFFAIRS, COLLABORATIVE TECHNIQUES, DEFENSE SYSTEMS, DETERRENCE, ESPIONAGE, FEDERAL BUDGETS, HACKING(COMPUTER SECURITY), INFORMATION ASSURANCE, INFORMATION SYSTEMS, INTELLIGENCE, INTERNET, INTRUSION DETECTION(COMPUTERS), NATIONAL SECURITY, NETWORK ARCHITECTURE, POLICIES, TEAMS(PERSONNEL), TERRORISTS, THESES, VULNERABILITY

Subject Categories : Government and Political Science
Sociology and Law
Computer Systems Management and Standards

Distribution Statement : APPROVED FOR PUBLIC RELEASE

Bibliographic Information

DEFENSE TECHNICAL INFORMATION CENTER

Select Search | Keywords

Accession Number : ADA620564

Title : Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to Support the DHS Cyber Security Mission

Descriptive Note : Master's thesis

Corporate Author : NAVAL POSTGRADUATE SCHOOL MONTEREY CA

Personal Author(s) : Lowery, Edward W

Full Text : http://www.dtic.mil/get-tr-doc/pdf?AD=ADA620564

Report Date : Dec 2014

Pagination or Media Count : 139

Abstract : Following the 9/11 terror attacks, the Department of Homeland Security (DHS) was mandated to ensure the security of the nation's cyber-supported critical infrastructure, which is predominantly privately owned and outside of the control of the U.S. government. This thesis examines the development of the government's cyber-security policies and primary operational entities through their lawful authorities and capabilities. The thesis also examines and contrasts the effectiveness of DHS's technology-centric, cyber-security approach, the deterrent effect realized through law enforcement cyber operations, and the suitability and effectiveness of the utilization of military or intelligence agencies, specifically the FBI, National Security Agency or Department of Defense, to fulfill the nation's domestic cyber-security mission. Evidence suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information-sharing programs, and develop cyber incidence response teams while not fully utilizing the U.S. Secret Service's legal authorities and capabilities in furtherance of the department's mission. Recommendations are offered to develop a whole-of-government cyber-security policy for an effective, integrated, cyber-security operation through the utilization of agency-specific authorities and capabilities, while protecting our nation's critical infrastructure and our citizens civil liberties.

Descriptors : *COMPUTER NETWORK SECURITY, *HOMELAND SECURITY, CIVIL AFFAIRS, COLLABORATIVE TECHNIQUES, DEFENSE SYSTEMS, DETERRENCE, ESPIONAGE, FEDERAL BUDGETS, HACKING(COMPUTER SECURITY), INFORMATION ASSURANCE, INFORMATION SYSTEMS, INTELLIGENCE, INTERNET, INTRUSION DETECTION(COMPUTERS), NATIONAL SECURITY, NETWORK ARCHITECTURE, POLICIES, TEAMS(PERSONNEL), TERRORISTS, THESES, VULNERABILITY

Subject Categories : Government and Political Science
Sociology and Law
Computer Systems Management and Standards

Distribution Statement : APPROVED FOR PUBLIC RELEASE

Subject Information/Abstract

DEFENSE TECHNICAL INFORMATION CENTER

Select Search | Keywords

Accession Number : ADA620564

Title : Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to Support the DHS Cyber Security Mission

Descriptive Note : Master's thesis

Corporate Author : NAVAL POSTGRADUATE SCHOOL MONTEREY CA

Personal Author(s) : Lowery, Edward W

Full Text : http://www.dtic.mil/get-tr-doc/pdf?AD=ADA620564

Report Date : Dec 2014

Pagination or Media Count : 139

Abstract : Following the 9/11 terror attacks, the Department of Homeland Security (DHS) was mandated to ensure the security of the nation's cyber-supported critical infrastructure, which is predominantly privately owned and outside of the control of the U.S. government. This thesis examines the development of the government's cyber-security policies and primary operational entities through their lawful authorities and capabilities. The thesis also examines and contrasts the effectiveness of DHS's technology-centric, cyber-security approach, the deterrent effect realized through law enforcement cyber operations, and the suitability and effectiveness of the utilization of military or intelligence agencies, specifically the FBI, National Security Agency or Department of Defense, to fulfill the nation's domestic cyber-security mission. Evidence suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information-sharing programs, and develop cyber incidence response teams while not fully utilizing the U.S. Secret Service's legal authorities and capabilities in furtherance of the department's mission. Recommendations are offered to develop a whole-of-government cyber-security policy for an effective, integrated, cyber-security operation through the utilization of agency-specific authorities and capabilities, while protecting our nation's critical infrastructure and our citizens civil liberties.

Descriptors : *COMPUTER NETWORK SECURITY, *HOMELAND SECURITY, CIVIL AFFAIRS, COLLABORATIVE TECHNIQUES, DEFENSE SYSTEMS, DETERRENCE, ESPIONAGE, FEDERAL BUDGETS, HACKING(COMPUTER SECURITY), INFORMATION ASSURANCE, INFORMATION SYSTEMS, INTELLIGENCE, INTERNET, INTRUSION DETECTION(COMPUTERS), NATIONAL SECURITY, NETWORK ARCHITECTURE, POLICIES, TEAMS(PERSONNEL), TERRORISTS, THESES, VULNERABILITY

Subject Categories : Government and Political Science
Sociology and Law
Computer Systems Management and Standards

Distribution Statement : APPROVED FOR PUBLIC RELEASE

Full-Text Document – Document Cover

NAVAL
POSTGRADUATE
SCHOOL
MONTEREY, CALIFORNIA

THESIS

CLOSING THE CYBER GAP: INTEGRATING
CROSS-GOVERNMENT CYBER CAPABILITIES
TO SUPPORT THE DHS CYBER SECURITY MISSION

by

Edward W. Lowery

December 2014

Thesis Advisor: Kathleen Kiernan
Co-Advisor: Lauren Fernandez

Approved for public release; distribution is unlimited

Document Details – Standard Form 298 Report Documentation Page

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis
4. TITLE AND SUBTITLE CLOSING THE CYBER GAP: INTEGRATINGCROSS-GOVERNMENT CYBER CAPABILITIESTO SUPPORT THE DHS CYBER SECURITY MISSION		**5. FUNDING NUMBERS**
6. AUTHOR(S) Edward W. Lowery		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Following the 9/11 terror attacks, the Department of Homeland Security (DHS) was mandated to ensure the security of the nation's cyber-supported critical infrastructure, which is predominantly privately owned and outside of the control of the U.S. government. This thesis examines the development of the government's cyber-security policies and primary operational entities through their lawful authorities and capabilities. The thesis also examines and contrasts the effectiveness of DHS's technology-centric, cyber-security approach, the deterrent effect realized through law enforcement cyber operations, and the suitability and effectiveness of the utilization of military or intelligence agencies, specifically the FBI, National Security Agency or Department of Defense, to fulfill the nation's domestic cyber-security mission.

Evidence suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information-sharing programs, and develop cyber incidence response teams while not fully utilizing the U.S. Secret Service's legal authorities and capabilities in furtherance of the department's mission.

Recommendations are offered to develop a whole-of-government cyber-security policy for an effective, integrated, cyber-security operation through the utilization of agency-specific authorities and capabilities, while protecting our nation's critical infrastructure and our citizens' civil liberties.

14. SUBJECT TERMS Cybersecurity, U.S. Secret Service, Department of Homeland Security, DHS	**15. NUMBER OF PAGES** 139
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

Discriptors: DTIC Thesaurus/Controlled Vocabulary

DTIC Thesaurus

The Thesaurus provides a broad multidisciplinary subject term vocabulary that aids in information search and retrieval. Subject terms, called Descriptors, are organized into hierarchies, where series of narrower terms are linked to broader terms. After performing a Thesaurus search, a user can insert a Descriptor directly into the Technical Reports search box located at the top of each page.

Search the DTIC Thesaurus

DTIC Thesaurus files for download:

DTIC Thesaurus in EXCEL, 11 May 2016
DTIC Thesaurus in HTML, 11 May 2016
DTIC Thesaurus in TXT, 11 May 2016
DTIC Thesaurus in XML, 11 May 2016
DTIC Thesaurus in SKOS TTL, 11 May 2016

DTIC Thesaurus Term Explanation

Terms of Use

- The DTIC Thesaurus is not copyrighted. No license is needed to use it.
- DTIC assumes no responsibility for any party's use or the results of such use of the DTIC thesaurus.
- Identify DTIC as the originator of the thesaurus, especially if disseminating a modified version of the original.
- The download does not guarantee your receipt of future updates.

If you have any questions or need assistance downloading this product, contact: dtic.belvoir.ecm.mbx.sources@mail.mil

Open Government at DTIC OPEN GOV

Thesaurus Search

In This Section

- DTIC Thesaurus Home
- About Thesaurus
- Subject Categories
- Alphabetical View
- Term Explanation
- Download
- Suggest Thesaurus Terms

DTIC Thesaurus

from Public Technical Reports Thesaurus

The thesaurus provides a broad, multidisciplinary subject-term vocabulary that reduces the need to search multiple synonyms. Subject terms, called Descriptors, are organized into hierarchies, where narrower terms are linked to broader terms.

Enter a descriptor:

cyber

Search | Clear Query

DTIC welcomes contributions to the thesaurus.

Thesaurus Results

Search

1. **CYBER** DEFENSE TECHNIQUES
2. COMPUTER SECURITY TECHNIQUES
3. MOVING TARGET DEFENSE
4. DEFENSE IN DEPTH

DTIC Thesaurus Entry

Descriptor	CYBER DEFENSE TECHNIQUES
Broader Terms:	COMPUTER SECURITY TECHNIQUES
Narrower Terms:	DEFENSE IN DEPTH MOVING TARGET DEFENSE
Related Terms:	

Subject Category Codes/Fields and Groups

In This Section

- DTIC Thesaurus Home
- About Thesaurus
- Subject Categories
- Alphabetical View
- Term Explanation
- Download
- Suggest Thesaurus Terms

Subject Categories

DTIC® has identified 25 broad subject fields and 251 groups to categorize the areas of scientific and technical interest. These fields and groups provide the structure for the subject grouping of technical reports in DTIC's collection and are used to define the areas of need-to-know in distributing these reports. Through this site, you will find the subject coverage for each subject category, as well as cross-references to related fields and groups.

01. Aviation Technology
02. Agriculture
03. Astronomy and Astrophysics
04. Atmospheric Sciences
05. Behavioral and Social Sciences
06. Biological and Medical Sciences
07. Chemistry
08. Earth Sciences and Oceanography
09. Electrotechnology and Fluidics
10. Power Production and Energy Conversion (Nonpropulsive)
11. Materials
12. Mathematical and Computer Sciences
13. Mechanical, Industrial, Civil and Marine Engineering
14. Test Equipment, Research Facilities and Reprography
15. Military Sciences
16. Guided Missile Technology
17. Navigation, Detection and Countermeasures
18. Nuclear Science and Technology
19. Ordnance
20. Physics
21. Propulsion, Engines and Fuels
22. Space Technology
23. Biotechnology
24. Environmental Pollution and Control
25. Communications

Subject Categorization Guide for Defense Science & Technology

Alphabetical Index to the SCG, September 2009
Numeric Index to the SCG, September 2009

Hierarchical Display

01 – Aviation Technology

01	Aerodynamics	Flight characteristics and problems of full-scale or model aircraft and their components as they are affected by the dynamics of air; Flight testing and wind tunnel testing. Includes theoretical and experimental aerodynamics as applied to missiles, See 16/02/01, Guided Missile Dynamics, Configurations and Control Surfaces. For the behavior of spacecraft in air, see 22/03, Spacecraft Trajectories and Reentry. For the aerodynamics of ground structures, see 13/13, Structural Engineering and Building Technology.
02	Military Aircraft Operations	Military aircraft operations such as takeoff Operations and landing, air traffic, all weather and night flight, taxiing, approach, and inflight refueling; Flight safety; Ground safety; Aviation accident studies; Aircraft simulators and training devices. For missile operations, see Field 16, Guided Missile Technology. For spacecraft operations, See Field 22, Space Technology. For navigation and air traffic control, see 17/07/03, Air Navigation and Guidance.
03	Aircraft	Design, production, and maintenance of aircraft, aircraft components, and aircraft equipment; Structural studies of complete aircraft components such as airframes, bodies, and wings. Airworthiness; Crashworthiness; Aircraft damage assessment and vulnerability studies; effects of gunfire and blast on aircraft and flight equipment. For civilian aircraft, See 01/03/09, Civilian Aircraft. For specific types of aircraft, See subgroups 01/03/01 - 01/03/12. See also Field 16, Guided Missile Technology and Field 22, Space Technology.
03/01	Helicopters	Includes attack helicopters. For civilian helicopters, See 01/03/09, Civilian Aircraft.
03/02	Bombers	
03/03	Attack and Fighter Aircraft	
03/04	Patrol and Reconnaissance Aircraft	Includes observation aircraft.
03/05	Transport Aircraft	Includes tanker aircraft.
03/06	Training Aircraft	
03/07	V/STOL	
03/08	Gliders and Parachutes	Includes paragliders and kites, for both military and civilian applications.
03/09	Civilian Aircraft	Does not include aircraft modified for military use.
03/10	Pilotless Aircraft R.P.V.; Drones.	Includes full size aircraft when configured as drones.
03/11	Lighter-than-air Aircraft	Airships, blimps, dirigibles, balloons, for both civilian and military applications.
03/12	Research and Experimental Aircraft	Includes aerospace aircraft.
04	Flight Control and Instrumentation	Instruments, sensors, displays and recorders necessary for control and monitoring the flight of an aircraft; Cockpit and cabin display devices and onboard checkout systems; Onboard navigation display devices; Automatic pilots; Stability and control systems; Boundary layer control systems; Dynamic and static control devices. If the application of a flight control system is apparent, see the field where the application is treated. For devices used to compute flight times and headings, See 17/07/03, Air Navigation and Guidance.
05	Terminal Flight Facilities	Airports; Military air bases; Runways; Hangars; Ground refueling systems; Heliports; Aircraft handling and maintenance equipment; Taxiways; Parking aprons; Crash and fire facilities. For air traffic control systems, See 17/07/03, Air Navigation and Guidance.
06	Commercial and General Aviation	Civil aircraft operations, as described in 01/02. Also includes civil airport passenger and vehicle traffic studies.

Release/Distribution Statement

DEFENSE TECHNICAL INFORMATION CENTER

Select Search | Keywords

Accession Number : ADA620564

Title : Closing the Cyber Gap: Integrating Cross-Government Cyber Capabilities to Support the DHS Cyber Security Mission

Descriptive Note : Master's thesis

Corporate Author : NAVAL POSTGRADUATE SCHOOL MONTEREY CA

Personal Author(s) : Lowery, Edward W

Full Text : http://www.dtic.mil/get-tr-doc/pdf?AD=ADA620564

Report Date : Dec 2014

Pagination or Media Count : 139

Abstract : Following the 9/11 terror attacks, the Department of Homeland Security (DHS) was mandated to ensure the security of the nation's cyber-supported critical infrastructure, which is predominantly privately owned and outside of the control of the U.S. government. This thesis examines the development of the government's cyber-security policies and primary operational entities through their lawful authorities and capabilities. The thesis also examines and contrasts the effectiveness of DHS's technology-centric, cyber-security approach, the deterrent effect realized through law enforcement cyber operations, and the suitability and effectiveness of the utilization of military or intelligence agencies, specifically the FBI, National Security Agency or Department of Defense, to fulfill the nation's domestic cyber-security mission. Evidence suggests that DHS has consistently chosen to devote disproportionate budgetary resources to develop defensive technologies of questionable effectiveness, initiate redundant information-sharing programs, and develop cyber incidence response teams while not fully utilizing the U.S. Secret Service's legal authorities and capabilities in furtherance of the department's mission. Recommendations are offered to develop a whole-of-government cyber-security policy for an effective, integrated, cyber-security operation through the utilization of agency-specific authorities and capabilities, while protecting our nation's critical infrastructure and our citizens civil liberties.

Descriptors : *COMPUTER NETWORK SECURITY, *HOMELAND SECURITY, CIVIL AFFAIRS, COLLABORATIVE TECHNIQUES, DEFENSE SYSTEMS, DETERRENCE, ESPIONAGE, FEDERAL BUDGETS, HACKING(COMPUTER SECURITY), INFORMATION ASSURANCE, INFORMATION SYSTEMS, INTELLIGENCE, INTERNET, INTRUSION DETECTION(COMPUTERS), NATIONAL SECURITY, NETWORK ARCHITECTURE, POLICIES, TEAMS(PERSONNEL), TERRORISTS, THESES, VULNERABILITY

Subject Categories : Government and Political Science
Sociology and Law
Computer Systems Management and Standards

Distribution Statement : APPROVED FOR PUBLIC RELEASE

Public Access

DoD Public Access Search

As DoD prepares to implement Public Access, DTIC has provided a search to aid the public in the disc
articles that are alre
collection search. Re

previous

DoD Public Access Search

DoD Public Access

Search terms entered below will yield a subset list of journal articles from the DTIC Technical Reports database.

Enter a term to search the DTIC TR collection:

Search | Clear Query

DoD's Implementation of Public Access

s DoD prepares to implement Public Access, the search above is provided to aid the public in the discovery of journal articles hat are already part of the DTIC collection search. DoD's approach to Public Access will start with access to DoD-funded ournal articles and associated datasets in intramural basic research (research that is performed by DoD personnel), then move n to implement public access for contractor and grantee-performed work. Metadata from datasets will be forwarded to ata.gov.

n collaboration with the Department of Energy's Office of Scientific and Technical Information (OSTI), DoD has set up a rototype "DoD Public Access Search." This search includes an initial collection of published journal articles that refer to DoD unding. When DoD begins to receive manuscripts from authors of DoD-funded research, the manuscripts will be matched against the publishers' versions and combined citations will be shown.

Access DoD Public Access Search

Benefits to DoD

- Increased access to government-wide scholarly publications and scientific data, cost savings to DoD libraries
- Increased visibility of DoD research priorities
- Provide the necessary information to validate the results of the research
- Expand innovation through a better understanding of our taxpayer funded research
- Bolster the credibility of DoD-funded scientific findings

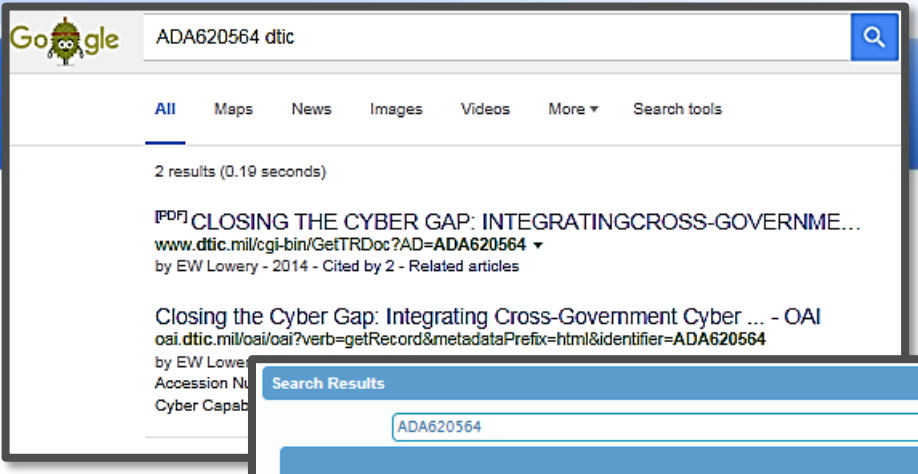
We welcome your input on additional articles to be added to the DoD collection.

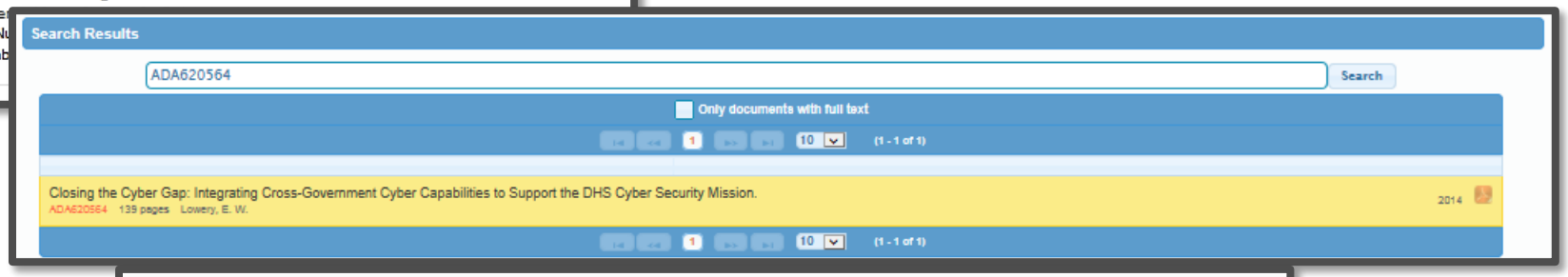
Additional Information:

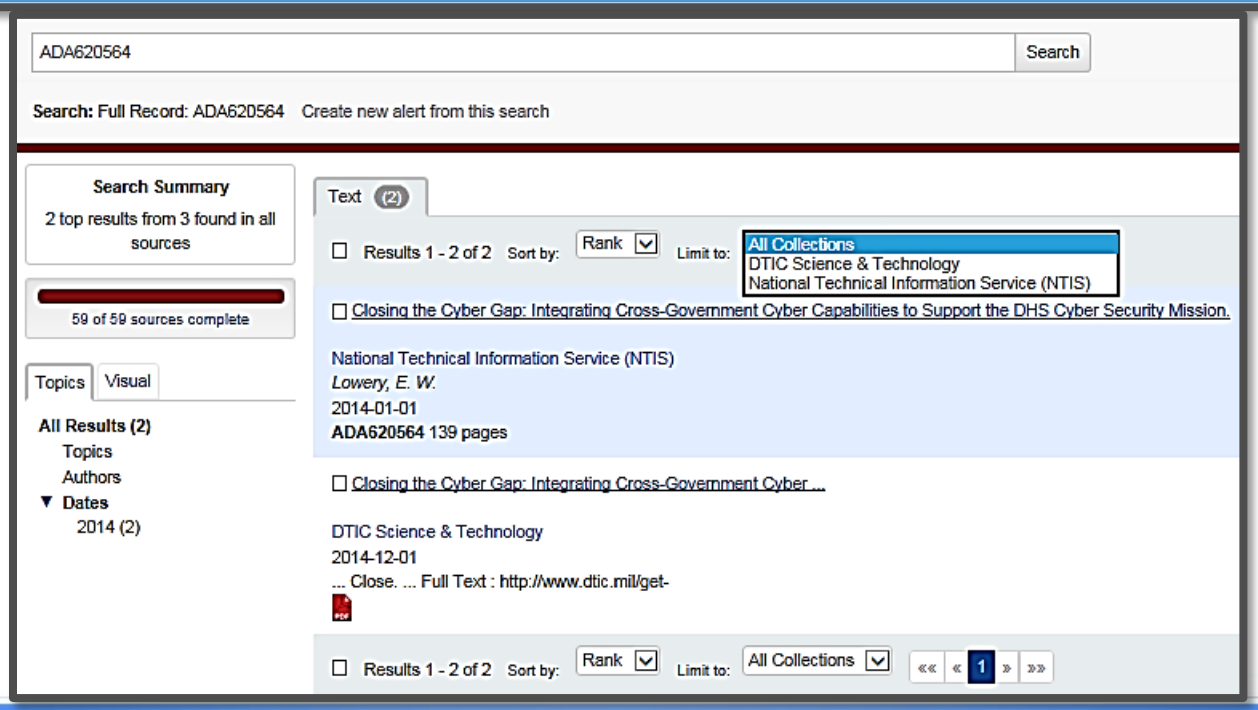
- "Increasing Access to the Results of Federally Funded Scientific Research." - 22 February 2013
- "Public Access to the Results of Department of Defense-Funded Research." - 9 Jul 2014
- "Department of Defense Public Access Plan" - Feb 2015
- "Public Access Plans for US Federal Agencies"
- "Data.gov"

For more information contact DTIC Public Access

Find Documents on Google, NTIS, & Science.gov







DoD Information Analysis Centers (IACs)

Begin your technical inquiry. The first 4 hours of research is free!

What are IAC Basic Centers of Operation (BCO)?

The Basic Centers of Operation (BCO) perform functions necessary to fulfill the mission and objectives applicable to the DoD Research, Development, Test and Evaluation (RDT&E) and acquisition communities' needs. These activities focus on the collection, analysis, synthesizing/processing and dissemination of Scientific and Technical Information (STI). The IAC Program has three MACs with different scope areas:

- **Cyber Security & Information Systems Information Analysis Center (CSIAC)**
- **Defense Systems Information Analysis Center (DSIAC)**
- **Homeland Defense Information Analysis Center (HDIAC)**

CSIAC
Cyber Security & Information Systems Information Analysis Center

DSIAC
Defense Systems Information Analysis Center

HDIAC
Homeland Defense & Security Information Analysis Center

"IACs serve as a proven resource for maximizing the value of each dollar the department spends."
Preferred Use of DoD IAC Contracts - Memo January 2015

IAC Technical Inquiries

What is a Technical Inquiry?

The IAC BCOs provide up to four free hours of information services, including literature searches, product/document requests and analysis within their focus areas. The information services are provided through their extensive database collections and subject matter expert (SME) networks which includes retired senior military leaders, leading academic researchers, and industry executives.

Examples of Technical Inquiries

Examples of technical inquires may include (but are not limited to):

- Analytical research in any of the IAC BCO focus areas. For example, request analytical research on a particular weapon system, biological agent, method of alternative energy, etc.
- Information on current technologies, industry standards and/or testing on advanced materials, sensing capabilities, modeling and simulation, or any of the IAC BCO focus areas.
- Analysis to identify potential capability gaps in any of the IAC BCO focus areas.

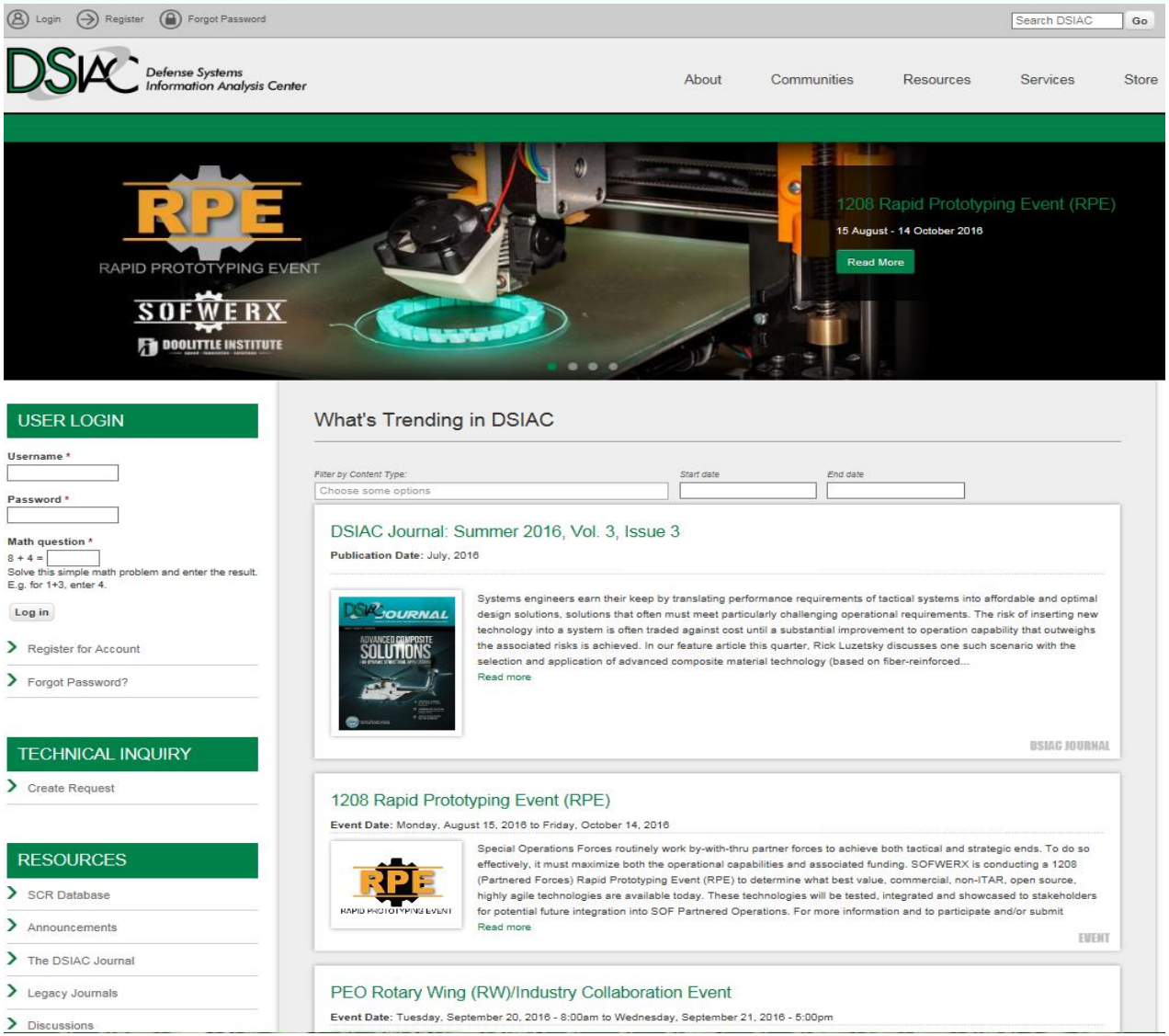
How to Get Started

Click on begin a technical inquiry with the desired IAC in the table below. The first 4 hours of research is free!

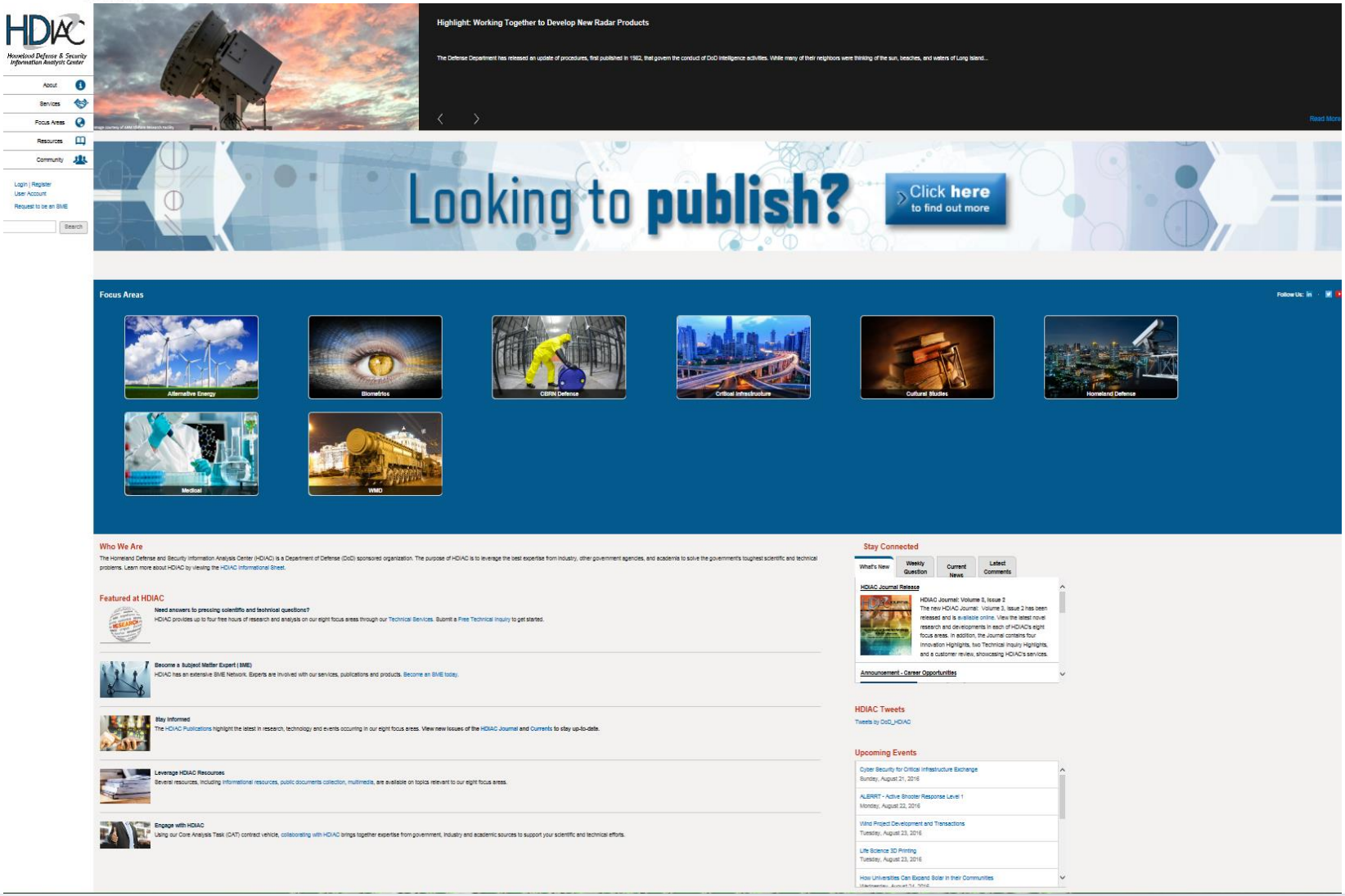
CSIAC Cyber Security & Information Systems Information Analysis Center	**Cyber Security & Information Systems Information Analysis Center (CSIAC)** -Software Data & Analysis, Information Assurance (IA), Modeling and Simulation (M&S) and Knowledge Management & Information Systems. **Begin a technical inquiry**
DSIAC Defense Systems Information Analysis Center	**Defense Systems Information Analysis Center (DSIAC)** - Weapons Systems; Autonomous Systems; Survivability and Vulnerability; Reliability, Maintainability, Quality, Supportability, and Interoperability (RMQSI); Advanced Materials; Military Sensing; Energetics; Directed Energy; Non-lethal Weapons. **Begin a technical inquiry**
HDIAC Homeland Defense & Security Information Analysis Center	**Homeland Defense Information Analysis Center (HDIAC)** - Homeland Defense and Security; Critical Infrastructure Protection (CIP); Weapons of Mass Destruction (WMD); Chemical, Biological, Radiological, and Nuclear Defense; Biometrics; Medical; Cultural Studies; Alternative Energy. **Begin a technical inquiry**

Cyber Security & Information Systems IAC (CSIAC)

Defense Systems IAC (DSIAC)



Homeland Defense & Security IAC



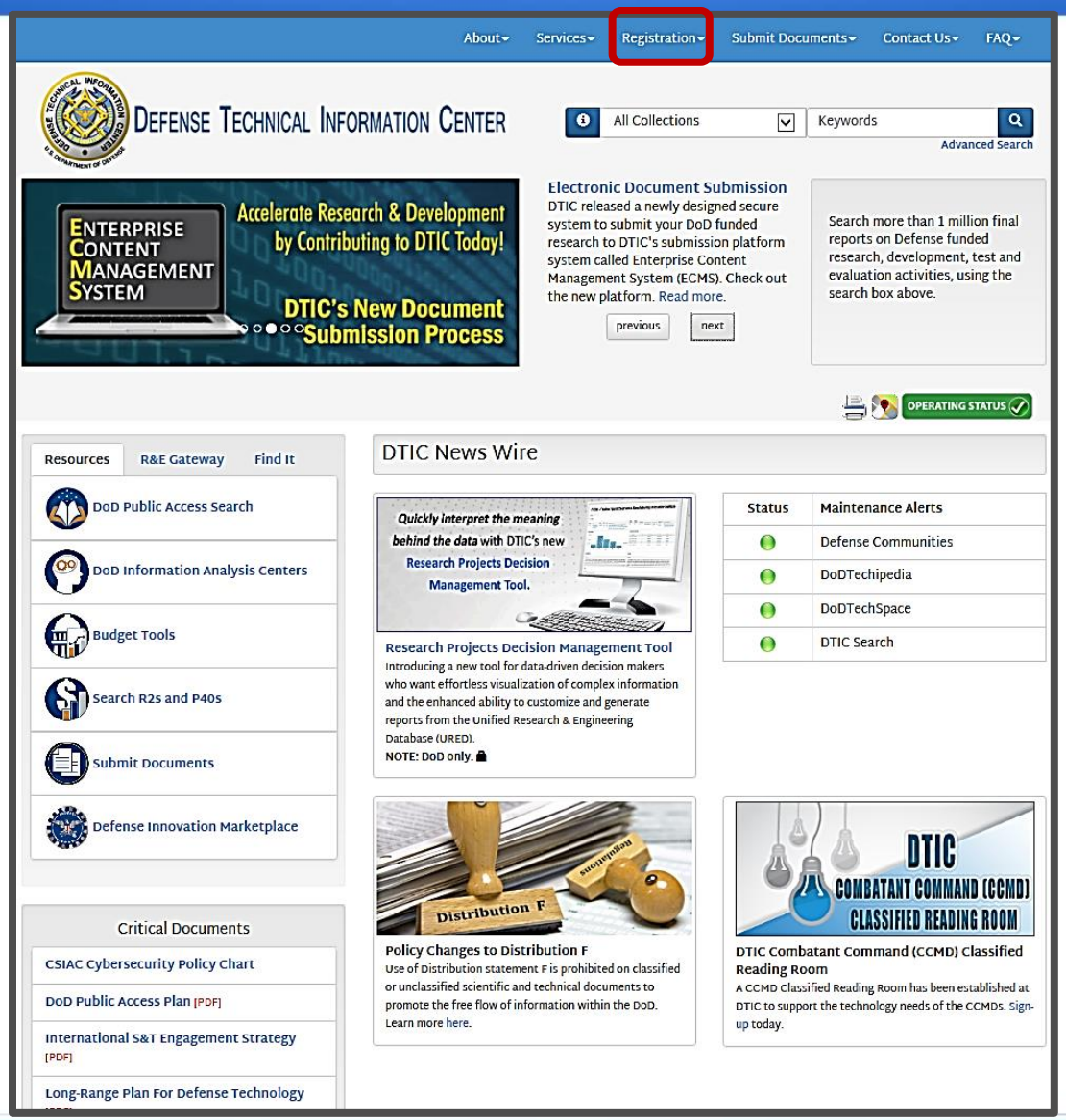
Strategies

- Discover technical information and experts in your subject area
- Find out who is funding RDT&E
- Find out who is performing the technical work
- Locate funding trends
- Keep up with technologies in your interest areas
- Build on existing research and don’t duplicate completed projects

Benefits of Registration

- Access controlled information
- Communicate in controlled environments
- Contribute your work electronically
- Eligible:
  - DoD
  - DoD contractors
  - Federal government
  - Federal government contractors

Registration: CAC, ECA, PIV



Secure Access

About Services Registration Submit Documents Contact Us FAQ

Contractor Employees
Government Employees
Security

CAL INFORMATION CENTER

Keywords

Advanced Search

OPERATING STATUS

DTIC Registration

NOTICE - **DTIC is modifying registration to accept PKI on all secured websites.** These changes are in support of a policy change established by the DoD Chief Information Officer (CIO), which was initiated to ensure a more secure, efficient, and effective DoD IT environment. The goal is to eliminate userid and password access.

Access to DTIC's secured websites requires the following:

- DoD Common Access Card (CAC)
- Personal Identity Verification (PIV): DTIC is now accepting federal government Personal Identity Verification (PIV) acces
- External Certification Authority (ECA): Full Operational Capability. For more information on how to obtain an ECA visit the following three sites:
  - Identrust - http://www.identrust.com/certificates/eca/
  - Symantec - http://www.symantec.com/page.jsp?id=eca-certificates
  - ORC - https://eca.orc.com/

DTIC's products and services are available to:

- Authorized U.S. DoD/Military employees
- Authorized U.S. government employees
- Authorized U.S. government contractors and subcontractors

Register Now

Adding DoD Root Certificates into your browser for CAC, ECA and PIV access.

Change your password Option to change your password will be turned off in the near future as DTIC moves to CAC/ECA/PIV access methods.

Contact DTIC's Registration Team for assistance with:

- Registration eligibility requirements
- Problems with accessing DTIC Web services
- Upgrading your account to a higher level of access than originally granted

If you have a SIPRNet account you can now register and access DTIC's classified sites on the SIPRNET. Visit https://reg.dtic.smil.mil/SDTICreg to register. Please contact the Customer Access Team for additional information at: 703-767 8273 or email: dtic.belvoir.us.mbx.dtic-access@mail.mil.

NOTICE - **Enterprise Email Change:** DTIC uses the email address that is on your CAC for your access to our controlled sites an for our communication with you. If your email address changes to a "mail.mil" address, you might have access issues for our systems and your groups within these systems or you might be missing messages from DTIC

Contractor Access & More…

Contractor Employees

Registration instructions for US Department of Defense (DoD) Federal Government contractors, Small Business Innovation & Research Program (SBIR), Historically Black Colleges or University (HBCU) or University Research Support (URS)/University Research Institutions (URI)); MUST have an active Government Contract or Grant.

The level of access granted to a contractor depends upon the classification of the contract or grant being registered with DTIC and the approval of the Government Approving Official (GAO), (i.e., Contracting Officer (CO), Contracting Officer Representative (COR), Contracting Officer Technical Representative (COTR), or Program Manager (PM)).

Contractors could have access to the following classifications depending on the level of their contract with GAO approval:

- Unclassified, Limited (UL)
- Confidential
- Secret
- Restricted Data
- Critical Nuclear Weapons Design Information (CNWDI/Restricted Data)

Contractors MUST register with a DoD Issued CAC, ECA cards/certs or Federal Government PIV, which is not the same as a PIV-I. Please contact DTIC registration staff dtic.belvoir.us.mbx.dtic-access@mail.mil with questions about user ID and password access.

Note: In order to register with a PIV card or ECA, DoD Root Certificates must be loaded to your browser. Please use the following URL to download the DoD Root certificates to your browser: http://www.dau.mil/faq/pages/dodcerts.aspx

Authorized ECA Vendors:

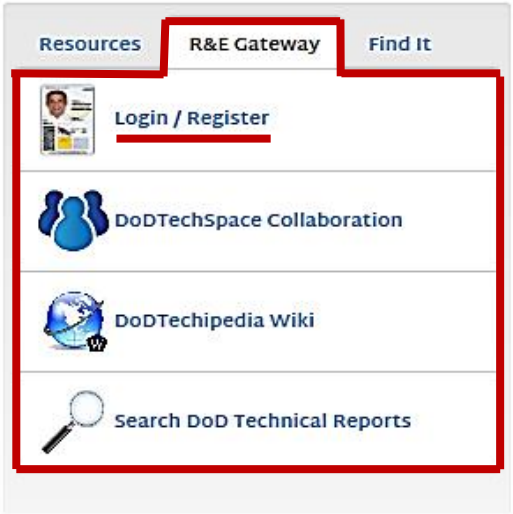
- IdenTrust https://identrust.com/certificates/eca/index.html
- ORC https://eca.orc.com/
- Symantec http://www.symantec.com/page.jsp?id=eca-certificates

Register Now

- Register as DoD/US Government Contractor
- Government Approving Officials (GAOs)
- Renew Your Registration
- Update User Information

R&E Gateway


DEFENSE TECHNICAL INFORMATION CENTER
All Collections
DTIC
EXCHANGE
NEWSLETTER
SPECIAL EDITION
Special Edition eXchange Newsletter
Get a "sneak peek" behind the scenes to DTIC's products enhancements and developments. Read this Special Edition of DTIC eXchange to learn more.
previous
next


Resources
R&E Gateway
Find It
Login / Register
DoDTechSpace Collaboration
DoDTechipedia Wiki
Search DoD Technical Reports


DTIC News Wire
DTIC's new Research Projects Decision Management Tool converts complex data to easily digestible visual information.
Research Projects Decision Management Tool
Introducing a new tool for data-driven decision makers who want effortless visualization of complex information and the enhanced ability to customize and generate reports from the Unified Research & Engineering Database (URED).
NOTE: DoD only.
Status

DTIC Registration/Login

R&E Gateway
POWERED by DTIC

DTIC's mission is to provide essential technical RDT&E information rapidly, accurately and reliably to support our DoD customers' needs.

Login Options

Smart Card Access Only

Log In

DoD CAC, DoD ECA Certificate, PIV Card

Login with Password

Continue...

No account yet? Register now...

If you have questions or need assistance, email dtic.belvoir.us.mbx.dtic-access@mail.mil or telephone DTIC's Customer Access Team at: 1-800-225-3842 (Menu Selection 2) or (703) 767-8273 or DSN 427-8273.

Classified Reading Room

COMBATANT COMMAND (CCMD)
CLASSIFIED READING ROOM

A complimentary and one-of-a-kind, access-controlled room
Exclusively located within the U.S. Department of Defense's Defense Technical Information Center Headquarters

Overview:

Admission is restricted to cleared industry/government/ DoD personnel with potential technology solutions to meet the mission requirements of the CCMDs.

The access-controlled room features two workstations for viewing sensitive CCMD capability needs.

User Benefits:

Gain invaluable insights on the top priorities and current capability demands of the CCMDs.

The requirements provided by participating CCMDs are current—within six (6) months.

Access Requirements:

Authorized industry/ government/DoD personnel must submit an application to visit the CCMD Classified Reading Room located within the DTIC Headquarters in Fort Belvoir, Virginia.

Applicants must have an active security clearance of SECRET or higher and be a U.S. citizen.

Application Process:

- Download and complete the application form at http://go.usa.gov/cJeVA
- Applications must be received 10 business days in advance of desired appointment date
- DTIC will verify applicant's security access
- CCMDs will review and approve applicant's request to view their respective classified capability needs
- DTIC will notify applicant and coordinate the visit appointment
- Appointments can be made for Tuesdays, Wednesdays and Thursdays only

Learn more and download the application form at:

http://go.usa.gov/cJepB

Questions?

Email: dtic.belvoir.pm.mbx.ReadingRoom@mail.mil

For other products and services offered by DTIC, visit:

http://www.dtic.mil

Support Challenging Technology Needs
of Current and Future Warfighters

Points of Contact

Wendy Hill
703-767-8225
DSN: 427-8225
Wendy.S.Hill.civ@mail.mil

http://www.dtic.mil
Access: reghelp@dtic.mil
Email our Reference team:
dtic.belvoir.us.mbx.reference@mail.mil
Call 1-800-CAL-DTIC (1-800-225-3842) or 703-767-8274 or DSN 427-8274 Monday through Friday from 7:00 a.m. - 5:00 p.m. Eastern time.

Disclaimer of Endorsement

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

August 2016

DoD SBIR Solicitation Page

U.S. Department of Defense
SMALL BUSINESS INNOVATION RESEARCH
SMALL BUSINESS TECHNOLOGY TRANSFER

Home | About | *for* Small Business | *for* Government | Awards | Contacts

Home » *for* Small Business » Current Solicitations

- *for* Small Business
- Program Descriptions
- Getting Started on Phase I
- Eligibility
- Solicitation Schedule
- Current Solicitations
- Topic Q&A (SITIS)
- Topic Search
- Proposal Submission
- Process Acceleration
- Resources for Small Businesses
- Phase III Concerns

Current Solicitations

In accordance with the Government Paperwork Elimination Act (GPEA) all DoD SBIR and STTR solicitations have been available in electronic format only from the DoD SBIR/STTR website.

- Click **here** to view the schedule for solicitations.
- Click **here** to view the complete solicitations archive.

SBIR Solicitation 2016.2
This solicitation is **CLOSED**
DARPA SBIR Topic SB162-009 will close on July 6, 2016 at 6:00 a.m. ET

STTR Solicitation 2016.B
This solicitation is **CLOSED**

DOD SBIR/STTR ANNOUNCEMENT LISTSERV

Join our **Listserv** to receive information on SBIR/STTR solicitations and events.

http://www.acq.osd.mil/osbp/sbir/solicitations/index.shtml

Solicitation Archive

U.S. Department of Defense
SMALL BUSINESS INNOVATION RESEARCH
SMALL BUSINESS TECHNOLOGY TRANSFER

Home | About | *for* Small Business | *for* Government | Awards | Contacts

Home » *for* Small Business » Current Solicitations » Past Solicitations

- *for* Small Business
- Program Descriptions
- Getting Started on Phase I
- Eligibility
- Solicitation Schedule
- **Current Solicitations**
- Topic Q&A (SITIS)
- Topic Search
- Proposal Submission
- Process Acceleration
- Resources for Small Businesses
- Phase III Concerns

Past Solicitations

> > > >

Fiscal Year	Solicitation	Close Date
FY16	SBIR Solicitation 2016.2	June 22, 2016
	STTR Solicitation 2016.B	June 22, 2016
	SBIR Solicitation 2016.1	February 17, 2016
	STTR Solicitation 2016.A	February 17, 2016
FY15	SBIR Solicitation 2015.3	October 28, 2015
	STTR Solicitation 2015.C	October 28, 2015
	SBIR Solicitation 2015.2	June 24, 2015
	STTR Solicitation 2015.B	June 24, 2015
	SBIR Solicitation 2015.1	February 25, 2015
	STTR Solicitation 2015.A	February 25, 2015
FY14	SBIR Solicitation 2014.3	October 22, 2014
	STTR Solicitation 2014.B	October 22, 2014
	SBIR Solicitation 2014.2	June 25, 2014
	STTR Solicitation 2014.A	March 9, 2014
	SBIR Solicitation 2014.1	January 22, 2014
FY13	SBIR Solicitation 2013.3	September 25, 2013
	STTR Solicitation 2013.B	September 25, 2013

DOD SBIR/STTR ANNOUNCEMENT LISTSERV

Join our Listserv to receive information on SBIR/STTR solicitations and events.

Solicitation topics

- *for* Small Business
- Program Descriptions
- Getting Started on Phase I
- Eligibility
- Solicitation Schedule
- **Current Solicitations**
- Topic Q&A (SITIS)
- Topic Search
- Proposal Submission
- Process Acceleration
- Resources for Small Businesses
- Phase III Concerns

DoD 2016.2 SBIR Solicitation

This solicitation is **CLOSED.**
DARPA SBIR Topic SB162-009 will close on July 6, 2016 at 6:00 a.m. ET

IMPORTANT NOTE: In addition to following the DoD-wide instructions in the DoD Program Solicitation, proposers must also follow the Component-specific instruction for the Component to which they are applying—see table below.

	June 8, 2016 NOTE: DARPA SBIR Topic SB162-009 has been amended to include the Certification for Applicants that are Majority-Owned by Multiple Venture Capital Operating Companies, Hedge Fund or Private Equity Firms
	June 8, 2016 NOTE: DARPA is accepting proposals from firms that are majority-owned by multiple venture capital operating companies in addition to other eligible firms. This authority ONLY applies to topic SB162-009 and supersedes Section 4.4 of the DoD SBIR FY16.2 Program Solicitation. The solicitation closing time for this topic has been extended to July 6, 2016 at 6:00 a.m. ET. In addition, the online SITIS Q&A System will be available for submission of technical questions for topic SB162-009 ONLY until June 22, 2016, at 12:00 Midnight ET.
	May 5, 2016 NOTE: OSD SBIR Topic OSD162-001 has been removed from this solicitation. In addition, the OSD SBIR 16.2 Phase I Instructions have also been removed.
	April 26, 2016 NOTE: Topics OSD162-006X and OSD162-007X have been added to the OSD 16.2 Direct to Phase II document.

Component Topics	Last Modified	Format		
		HTML	PDF	MS WORD
DoD Instructions: 2016.2 SBIR	May 23, 2016	HTML	PDF	DOC
Army	May 23, 2016	HTML	PDF	DOC
Navy	May 23, 2016	HTML	PDF	DOC
Air Force	May 23, 2016	HTML	PDF	DOC
Air Force Direct to Phase II	May 23, 2016	HTML	PDF	DOC
DARPA	June 8, 2016	HTML	PDF	DOC
DARPA Direct to Phase II	June 8, 2016	HTML	PDF	DOC
DLA	May 23, 2016	HTML	PDF	DOC

SCHEDULE CHANGES

IMPORTANT DATES

April 22, 2016
Solicitation enters pre-release

May 23, 2016
Solicitation opens and DoD begins accepting proposals

June 8, 2016
SITIS closes to new questions

June 22, 2016
Solicitation closes to receipt of proposals at 6:00 AM ET—*plan ahead and submit early.*

June 22, 2016
DARPA SB162-009 SITIS closes to new questions

July 6, 2016
DARPA SB162-009 closes to the receipt of proposals at 6:00 AM ET

DOD SBIR/STTR ANNOUNCEMENT LISTSERV

Join our Listserv to receive information on SBIR/STTR solicitations and events.

SBIR Gateway

Zyn Systems

SBIR Gateway — SBIR Information on Solicitations, Grants and Conferences

Far West Region FLC Federal Laboratory Consortium — FLC Far West Region

Mid-Continent Region FLC Federal Laboratory Consortium — FLC Mid-Continent Region

Navy SBIR Program

2007 Tibbetts Awards

Zyn Systems — Zyn Systems

p://www.zyn.com

Links to Federal Agency SBIR/STTR Content

SBIR Gateway

Your Easy to Use SBIR Information Site

SBIR Open Topic Search via SBIR.gov

Resources

- SBIR Insider Newsletter
- Solicitation Dates
- SBIR Agency Links
- SBIR Events Calendar
- SBA FAST Awardees
- About SBIR Funding
- Federal Laboratories
- SBIR Policy Directive
- Contact Us

News Items

Latest SBIR *Insider* News
Updated 3/21/16

Updated Solicitation Schedule
Updated 6/26/16

SBIR News Archive

2012 NDAA
SBIR Reauthorization Law

National / Regional Conferences

18th Annual NIH National SBIR/STTR Conference
Orlando FL * November 15-17, 2016

SBIR/STTR Innovation Summit
Austin, TX November 29 - December 1, 2016

View SBIR Conference Calendar
Includes State & Regional Events

Search Services

Open SBIR/STTR Solicitation Topics
Via SBIR.gov

Closed SBIR/STTR Solicitation Topics
Topics often *recycled* for future solicitations

Past SBIR/STTR Awards
SBIR/STTR Awards Databases

Federal Laboratory R&D Resources
Keyword search for federal tech resources

Help & Assistance Services

State & Local Assistance Services
They're here to help you

3rd Party Assistance Services
Non-Government *for profit* services

http://www.zyn.com/sbir

SBIR Federal Agency Program Links

Dept. of Agriculture:
USDA SBIR Home Page

Dept. of Commerce:
DOC-NOAA SBIR Page
DOC-NIST Home Page

Dept. of Defense:
DOD SBIR Home Page
Air Force SBIR/STTR
Army SBIR/STTR
Navy SBIR/STTR

CBD - Chem-Bio Defense
DARPA SBIR Program Home Page
DHP - Defense Health Program
DLA - Defense Logistics Agency
DMEA - Defense Microelectronics Activity
DTIC-Defense Technical Information Center
DTRA - Defense Threat Reduction Agency
MDA SBIR Program Home Page
NGA - National Geospatial-Intelligence Agency
SOCOM-Special Operations Command

Dept. of Education:
ED IES
ED OSERS / NIDDR

Dept. of Energy:
DOE SBIR Home Page

Dept. of Health & Human Services
NIH SBIR Home Page

Dept. of Homeland Security
DHS S&T Directorate
DHS DNDO

Dept. of Transportation:
DOT SBIR Home Page

Environmental Protection Agency:
EPA SBIR Home Page

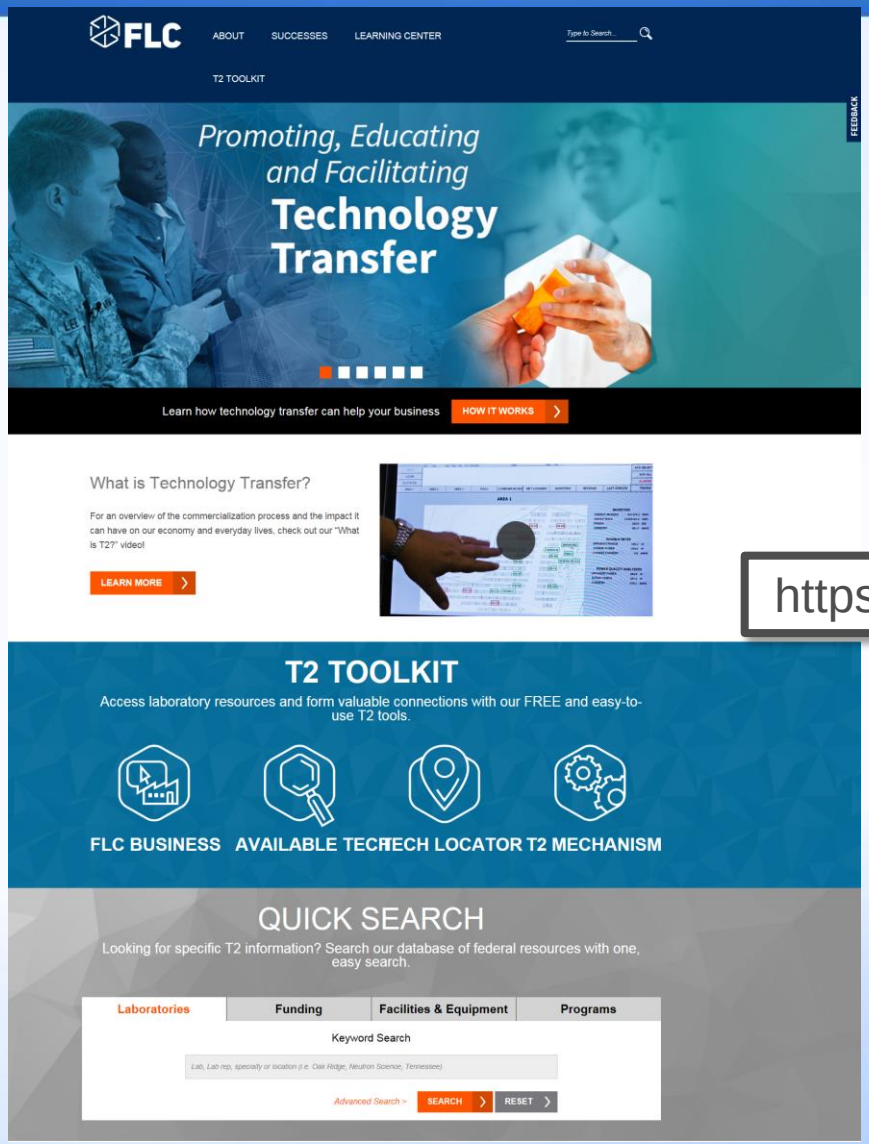
National Aeronautics & Space Administration:
NASA SBIR Home Page

National Science Foundation:
NSF SBIR Home Page

Small Business Administration:
SBA SBIR Home Page

SBIR.gov Portal
SBIR.gov

Federal Laboratory Consortium for Technology Transfer



https://www.federallabs.org