

Quantifying Security Costs

Class	Category	ActivityGroup	TreasuryCode	BACode	BudgetLineItem	ProgramIdentifier	ProgramElement	PartialPE	Comment	FY2016
-------	----------	---------------	--------------	--------	----------------	-------------------	----------------	-----------	---------	--------

Instructions

- 1) Department of Defense (DoD) Directive 5200.43 (Management of the Defense Security Enterprise of October 1, 2012) and the Defense Security Enterprise Strategic Plan require the quantification of security costs. This exhibit provides the framework for collecting security costs. The intent of this exhibit is to quantify the cost of security resources regardless of whether they are funded via security or non-security budgets or whether they support security in part or total.
- 2) Identify for each Category and associated Activity Group (AG) the resources (costs) by Treasury Code, Budget Activity (BA), Budget Line Item (BLI) and Program Element (PE) for fiscal year 2014 (actuals). NOTE: MIP, NIP, or any other funds associated with security expenditures should be used to quantify security related costs.
- 3) Indicate Yes or No if the identified PE funds other programs besides Security.
- 4) Utilize only those PE's that are associated with the following program identifiers (PIs) (1419-Security Services, 1549-Physical Security Equipment, 1596-Communications/Information Security, 1849-Personnel Security Investigations) located in CAPES's DoD Resources Data Warehouse (DRDW) database.
- 5) When identifying resources for Information Security, do not include costs for Special Access Program Security Measures, Military Construction, Manpower, and Training.
- 6) When identifying resources for Operations Security, do not include costs for Military Construction.
- 7) When identifying resources for Personnel Security, do not include costs for Suitability, Special Access Program Security Measures, Manpower, and Training.
- 8) When identifying resources for Physical Security, do not include costs for Chemical, Biological, Radiological or Nuclear-Specific Security Measures; Special Access Program Security Measures; Military Construction; Manpower; and Training.
- 9) When identifying resources for Security Training, do not include costs for Manpower.
- 10) Do not include any costs associated with security of the nuclear enterprise in this exhibit, including but not limited to nuclear storage areas, nuclear security sensor systems, access control systems that exist to support only nuclear-related areas, training related to nuclear security operations, specialized equipment including vehicles supporting nuclear security operations, and clearance and accountability systems and associated administrative requirements.
- 11) In the comment field identify the level of data obtained and/or the methodology used to determine costs.
- 12) Report \$ only once per Category, using the most appropriate AG.
- 13) Report costs \$ in Thousands (\$000).
- 14) Organizations required to support this exhibit are shown in SNaP Appendix A.
- 15) Note: To preclude Components/Defense Agencies from having to enter data twice, security costs identified in the DSE System and Investment List (maintenance cost only) and in the SNaP Combating Terrorism Detail exhibit will be pulled to support this exhibit. The following data fields will be extracted: DSE System and Investment List - Defense Central Index of Investigation (DCII), Improved Investigative Records Repository (iIRR), and Joint Personnel Adjudication System (JPAS); SNaP Combating Terrorism Detail - Barriers, Blast Mitigation, Communication, Explosive Detection, Intrusion Detection, Site Improvements, and Physical Security Research and Design.

Definitions

Class: (Closed List) System Field: Classification.

C: CONFIDENTIAL

C/NF: CONFIDENTIAL//NOFORN

F: FOR OFFICIAL USE ONLY

S: SECRET

S/NF: SECRET//NOFORN

U: UNCLASSIFIED

Category: (Closed List) The category for which security costs are grouped.

Information Security: The security discipline concerned with implementation of a system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information that is authorized protection by executive order, statute, or regulation. Information Security includes protection of information that is classified, controlled unclassified (CUI), and special compartmental information (SCI).

Operations Security (OPSEC): A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

Personnel Security: The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions.

Physical Security: Security concerned with physical measures designed to safeguard personnel, prevent unauthorized access to equipment installations, material, and documents, and defend them against espionage, sabotage, damage, and theft.

Security Training:

ActivityGroup: (Close List) A specified grouping that describes the resource supporting the security function. Refer to the security function and security resource relationship matrix.

Access National Agency Check and Inquiries (ANACI):

Badges/Credentials: A physical artifact issued by an authority for a lawful government purpose that attests to the possessor's right to logical and physical access to classified information or material, or controlled facilities, areas, or information.

Canines:

Central Adjudication Facility Administrative Costs: Include: subscriptions to personnel security-related databases (e.g., LexisNexis).

Central Adjudication Security Personnel Repository (CASPR): The DoD system for the management of personnel security investigation billing and payment functions. The system (administered by the Department of the Air Force) is the focal point for personnel security investigation projections, billing, invoicing, and payment functions (to include billing disputes and reconciliations). AIR FORCE ONLY

Collateral Areas: A secure area or vault accredited to process or store classified information at the confidential, secret, or top secret level. Include: open storage areas, closed storage areas, etc.

Continuous Evaluation: An investigative technique that leverages an automated records check methodology and applies standardized business rules to identify adjudicatively relevant information between investigations to assess cleared individuals' on-going eligibility for access to classified information.

Controlled Areas/Facilities: An installation, facility, or space where access restrictions apply and that require physical security measures to safeguard personnel, property, or material. Unless measures are applied to qualify the area as a restricted area, controlled areas are not required to meet physical security standards to allow open storage of classified material or protection of high-value items.

Defense Information System for Security (DISS): A family of systems composed of the Case Adjudication Tracking System (CATS), the Joint Verification System (JVS) and the Common Portal (a future development). CATS is the DoD non-Intelligence Community IT system for case management and adjudications. JVS is a system within DISS that provides the functionality for the maintenance and verification of security information. The DISS Portal will allow for reuse of IT services across the DoD Enterprise, communication with external interfaces, integrated CATS and JVS interfaces in each application template, ad-hoc reporting capabilities and a comprehensive business analytics function. Defense Security Service (DSS) ONLY

Fingerprint Scanners: Electronic fingerprint machines at Military Departments and DoD Components used to submit electronic fingerprints in support of background investigations.

Information Security Research and Design: Include: pilots, etc.

Keys, Locks, and Containers: Include key cards, locks, and locked containers used in support of Physical Security (i.e., arms, ammunition, and explosives).

Marine Mammal Program:

Marking Tools: Include: Titus Messaging Tool, etc.

National Agency Check with Inquiries (NACI):

National Agency Check with Local Agency Checks and Credit Check (NACLIC):

Operations Security Assessments and Surveys: Conducting OPSEC assessments and surveys of DoD organizations, activities and operations.

Operations Security Compliance and Assistance Services: Ensuring compliance and providing assistance with component and/or sub-component OPSEC policies, doctrine and procedures.

Operations Security Doctrine Development: Developing OPSEC tactics, techniques and procedures for planning, executing and assessing OPSEC.

Operations Security Execution and Assessment: Executing OPSEC across the range of military operations and assessing the effectiveness of OPSEC during all phases of military operations.

Operations Security Management: Planning and executing OPSEC activities in DoD components and sub-components.

Operations Security Planning: Planning OPSEC operations.

Operations Security Policy, Strategy and Integration Development: Producing, coordinating and disseminating DoD component and sub-component OPSEC policies and strategies for planning, executing and assessing OPSEC.

Operations Security Research, Development and Evaluation: Researching, developing, acquiring and using automated risk analysis tools to facilitate the OPSEC process.

Operations Security Resource Management: Planning, programming and budgeting and managing execution of resources for dedicated manpower and funding to carry out OPSEC responsibilities.

Other Personnel Security Investigation Costs: Include: enhanced subject interviews, expanded focus investigations or other issue resolutions, reopens, upgrades, cancellations, etc.

Personnel (INFOSEC, OPSEC, PERSEC, PHYSEC):

Personnel Security Research and Design: Include: pilots, etc.

Phased Periodic Reinvestigation (PPR):

Physical Security Equipment Systems: Include: access control points, access control systems, card readers, security-related signage/markings, non-permanent security structures, etc. Do NOT include: SCIF costs.

Physical Security Service Specific Courses: Include: classroom, onsite, etc.

Polygraph Instruments: A diagnostic instrument to measure and record respiration, electrodermal, blood volume, and heart rate responses to verbal or visual stimuli.

Recruiting Information Systems: Systems used by Military Departments to submit background investigations requests on persons accessioning into the military. Army: ARISS; Navy: NRISS; Marines: MCRISS; Air Force: AFRISS; Air Force Reserve: AFRRISS. These systems are individually updated/renewed by the respective commands as investigation submission requirements change. Include: personnel security upgrades only.

Review of Adjudicative Documentation, Accuracy and Rationales (RADAR): The consistent documentation of adjudicative decisions in CATS based on DoD policy especially as it relates to adjudicative determinations in cases with significant derogatory information. Adjudicative rationales are pushed from CATS to JPAS and are semi-annually aggregated and evaluated in a statistical measure to identify adjudicative quality. OUSD(I) ONLY

Secure Web Fingerprint Transmission (SWFT): A DSS storage and submission system for Industry submission of electronically captured fingerprint images. DSS ONLY

Single Scope Background Investigation (SSBI):

Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR):

Technical Surveillance Countermeasures (TSCM): Physical, electronic, and visual techniques used to detect and counter technical surveillance devices, technical security threats, and related physical security deficiencies.

TEMPEST Countermeasures: Include: RF film and foil, signal live filters, power line transformers, optical isolators, etc.

TreasuryCode: Treasury Code is a defined set of four-to-six digit numeric codes from the Comptroller that identifies resource types. The list of Treasury Code values can be found on the SNaP web site website by clicking the "Instructions" tab, then selecting the "Documents". (<https://snap.cape.osd.mil>).

BACode: (Closed List) Budget Activity is a two-digit identifier for the categories within each appropriation and fund account to identify the purposes, projects, or types of activities financed by the appropriation fund. The list of BA Codes and Titles can be found on the SNaP web site <https://snap.cape.osd.mil> by selecting the Instructions/Documents menu.

BudgetLineItem: (Closed List) The budget Line Item varies by the Appropriation group: O&M - provide the Activity Group (AG) and Sub-Activity Group (SAG); RDT&E - provide the Project Number; Procurement - provide the Line Item; and MILCON - provide the Project Number. The list of Budget Line Item/Budget Line Item Title values can be found on the SNaP web site <https://snap.cape.osd.mil> by selecting the Instructions/Documents menu.

ProgramIdentifier: (Closed List) The ProgramIdentifier is a 4-digit code that describes resources and processes required to support a platform, product, unit, or Department Activity of critical interest to the Future Years Defense Program (FYDP) community.

1419: 1419 Security Services

1549: 1549 Physical Security Equipment--RDT&E

1596: 1596 Comms/Information/Info System Security (Comsec/InfoSec/ISSP)

1849: 1849 Personnel Security Investigations

ProgramElement: The Program Element is a primary data element in the Future Years Defense Program (FYDP) and generally represents aggregations of organizational entities and related resources. The PE is up to ten-digits in length, a seven-digit numeric identifier followed by up to three-digits alphanumeric code for FYDP organizations. The list of Program Element codes and titles values can be found on the SNaP web site <https://snap.cape.osd.mil> by selecting the Instructions/Documents menu.

PartialPE: (Closed List) Identifies whether the identified PE funds other programs besides Security.

Comment: Identify the level of data obtained and/or the methodology used to determine costs.

Business Rules

- 1) N/A

DRAFT

Data Matrix: Org, ProgramIdentifier, ProgramElement Relationship

Org	ProgramIdentifier	ProgramElement
ARMY	1419	0208538A
		0208539A
		0528539A
		0538539A
	1596	0303140A
		0307665A
		0607664A
		0607665A
DIA	1596	0303401L
DISA	1596	0303135K
		0303140K
DSS	1596	0303140V
		0304130V
		0604130V
	1849	0305187V
NAVY	1419	0208047N
		0208147N
		0208347N
		0208538N
		0208539N
		0208547N
		0305134N
	1596	0303140N
		0503159N
NSA	1596	0303135G
		0303136G
		0303140G
OSD	1549	0603161D8Z
		0604161D8Z
	1596	0203345D8Z
		0303140D8Z
SOCOM	1419	1120464BB
		1120465BB
		1120466BB
		1120467BB

Org	ProgramIdentifier	ProgramElement
	1596	1133135BB
		1133401BB
USAF	1419	0108538F
		0108539F
		0207589F
		0208538F
		0208539F
		0305128F
		0305538F
		0305539F
		0408539F
		0502625F
		0505539F
		0603287F
		0604287F
		0708538F
		0708539F
		0805538F
		0805539F
		0808538F
		0808539F
		0908538F
	0908539F	
	1549	0603287F
	1596	0203345F
		0303135F
		0303140F
		0305128F
		0401845F
0503120F		
1849	0305128F	
	0305191F	
USMC	1419	0208538M
		0208539M
WHS	1849	0903430D8W

Data Matrix: Org, ProgramIdentifier Relationship

Org	ProgramIdentifier
ARMY	1419
	1596
DIA	1596
DISA	1596
DSS	1596
	1849
NAVY	1419
	1596
NSA	1596
OSD	1549
	1596
SOCOM	1419
	1596
USAF	1419
	1549
	1596
	1849
USMC	1419
WHS	1849

Data Matrix: Category, ActivityGroup Relationship

Category	ActivityGroup
Information Security	Collateral Areas
	Controlled Areas/Facilities
	Information Security Research and Design
	Marking Tools
	Technical Surveillance Countermeasures (TSCM)
	TEMPEST Countermeasures
Operations Security (OPSEC)	Operations Security Assessments and Surveys
	Operations Security Compliance and Assistance Services
	Operations Security Doctrine Development
	Operations Security Execution and Assessment
	Operations Security Management
	Operations Security Planning
	Operations Security Policy, Strategy and Integration Development

Category	ActivityGroup
	Operations Security Research, Development and Evaluation
	Operations Security Resource Management
Personnel Security	Access National Agency Check and Inquiries (ANACI)
	Central Adjudication Facility Administrative Costs
	Central Adjudication Security Personnel Repository (CASPR)
	Continuous Evaluation
	Defense Information System for Security (DISS)
	Fingerprint Scanners
	National Agency Check with Inquiries (NACI)
	National Agency Check with Local Agency Checks and Credit Check (NACLC)
	Other Personnel Security Investigation Costs
	Personnel (INFOSEC, OPSEC, PERSEC, PHYSEC)
	Personnel Security Research and Design
	Phased Periodic Reinvestigation (PPR)
	Polygraph Instruments
	Recruiting Information Systems
	Review of Adjudicative Documentation, Accuracy and Rationales (RADAR)
	Secure Web Fingerprint Transmission (SWFT)
	Single Scope Background Investigation (SSBI)
	Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR)
Physical Security	Badges/Credentials
	Canines
	Keys, Locks, and Containers
	Marine Mammal Program
	Physical Security Equipment Systems
Security Training	Physical Security Service Specific Courses

Subject Matter Experts: For questions regarding this exhibit, please submit a SIRS Functional issue in SNaP, or contact the Subject Matter Expert. A list of SMEs is available in SNaP by clicking the SME link on the Instructions/Data Requirements page.

Technical Issues: To report technical issues with the SNaP web site, please submit a SIRS Technical issue in SNaP, or contact the Technical Staff. A list of the SNaP Technical personnel is available on the SNaP Home page.