Central Intelligence Agency

Washington, D.C. 20505

6 March 2012

Mr. John P. Fitzpatrick, Director
Information Security Oversight Office
National Archives and Records Administration
Washington, D.C. 20408-0001

Dear Mr. Fitzpatrick: John

(U//FOUO) Enclosed is the Central Intelligence Agency's (CIA) Cost Estimate Report for Security Classification Activities for Fiscal Year 2011. We appreciate the extension of our deadline from the original date of 29 February. The increased expenditure for security classification activities reflects a strong commitment by the CIA to meet the significant challenges of securing classified information. The CIA continues to provide excellent protection of classified information and activities. We have sought and applied additional funding whenever possible to continue to enhance our handling of classified information.

(U) Please contact [redacted] Chief, Classification Management and Collaboration Group, at [redacted].

(b)(3)
(b)(6)
(b)(3)

Sincerely,

[redacted]

Director, Information Management Services

(b)(3)
(b)(6)

Enclosure

[redacted]

(b)(3)

Upon removal of attachment(s), this document is UNCLASSIFIED//FOUO

~~SECRET~~

Mr. John P. Fitzpatrick

[redacted] (b)(3)

Distribution:
Orig - Adressee
1 - CIO
2 - D/IMS
1 - C/CMCG
1 - [redacted] (b)(3) (b)(6)

SECRET

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Central Intelligence Agency	**Fiscal Year:** 2011

Point of Contact: (Name and phone number)		(b)(3) (b)(6)

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*		(b)(1) (b)(3) (b)(6)
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*		
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*		
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*		
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*		
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*		
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*		
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*		
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*		
TOTAL *(sum of items 1-9)*		

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.* (b)(3)

SECRET

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

   Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

   Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

   National Agency Check: Include only when used for basis for granting a clearance.

   Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

   Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

   Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

   Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

   Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

   Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

   Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

Approved for Release: 2021/04/06 C06810064

CLASSIFICATION: **UNCLASSIFIED**

(b)(3)

UNCLASSIFIED

Subject: (b)(3)
[AIN] Cost Report Received (b)(6)
To:

From: (b)(6)
Date: 03/06/2012 03:51 PM
Hide Details
From: (b)(6)

To: <STEPHARS@ucia.gov>

Please respond to (b)(6)

(b)(3)
(b)(6)

We have successfully received CIA's cost report for FY 2011.

Thanks,

(b)(6)

(b)(3)
(b)(6)

3/6/2012

(b)(6)

Program Analyst
Information Security Oversight Office
National Archives and Records Administration
Washington, DC

(b)(3)

(b)(3)
(b)(6)

3/6/2012