



**ENHANCING YOUR INTELLIGENCE AGENCY INFORMATION RESOURCES IQ:
PT. 7 ENERGY, HOMELAND SECURITY, STATE, AND TREASURY DEPTS., AND
BOARDS AND COMMISSIONS**

Professor Bert Chapman

Purdue University Libraries

FDLP Academy

March 26, 2019



Libraries



Office of
INTELLIGENCE AND COUNTERINTELLIGENCE



Job Opportunities

DOE Jobs and Internships

U.S. Intelligence Careers

DOE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

- Responsible for intelligence and counterintelligence activities throughout DOE with nearly 30 offices nationally.
- Protects vital national security information and technologies and intellectual property.
- Leverages DOE's scientific and technological expertise to support policymakers and national security missions in defense, homeland security, cyber security, intelligence, and energy security.
- Relevant DOE agencies include:
- National Nuclear Security Administration (NNSA)-Responsible for maintaining U.S. nuclear weapons stockpile, preventing WMD proliferation, providing the Navy with safe & effective nuclear propulsion, and responding to U.S. and foreign nuclear and radiological emergencies.
- National Laboratory System
- Various Washington headquarters offices and agencies e.g. Office of Cybersecurity, Energy Security, & Emergency Response



Vacancy Announcement 17-0001-10

Intelligence Analysis Directorate

The mission of the U.S. Department of Energy's **Office of Intelligence and Counterintelligence (DOE-IN)** is to identify and mitigate threats to U.S. national security and the DOE Enterprise, and inform national security decision making through scientific and technical expertise.

As a member of the DOE-IN team, you will play a key role in reducing the global security threat, strengthening the nuclear security infrastructure, and buttressing America's economic prosperity. You will join an unmatched team of experts in a wide variety of disciplines including nuclear weapons and material security, energy security, economics, science and technology, counterintelligence, threat assessment, investigations, and cyber. Our mission support functions offer opportunities for professionals with backgrounds in law, finance, engineering, human resources, and information management.

The role of DOE-IN's **Intelligence Analysis Directorate** is to provide leading-edge, scientifically-based and technically-sound foreign nuclear and energy security intelligence analysis that enables U.S. policy makers to address critical national security issues.

DOE-IN offers a stimulating and collegial work environment, with work assignments that are on the forefront of America's national security priorities.

The U.S. Department of Energy Office of Intelligence and Counterintelligence is a member of the [U.S. Intelligence Community](#). Most federal positions are within the Washington, D.C. area.

The Intelligence Analysis Directorate recruits for positions such as the following:

- **Energy Security Intelligence Analyst**
 - Research and provide intelligence analysis and support to DOE and other USG policymakers on energy and environmental security.
- **Nuclear Intelligence Analyst**
 - Research and provide intelligence analysis on critical nuclear security issues including foreign nuclear weapons, counterproliferation, nuclear terrorism, and nuclear materials security.

practices; development of tradecraft training plans and strategy; identification of intelligence gaps and production of multi-discipline collection requirements; and editorial, finished production, and dissemination technical support.

If you are interested in joining our organization, we are looking for highly skilled, motivated and talented Americans with relevant education and experience to join our team. Please [send us your resume](#).

Your resume will be retained in active status for 6 months. Candidates will be contacted if and when an interview is desired.

TRAVEL REQUIRED

- Variable. Typically 0 – 25%

RELOCATION AUTHORIZED

- No.

REQUIREMENTS INCLUDE:

- You must be a United States Citizen.
- This employer participates in the e-Verify program.
- See "Other Information" section regarding Selective Service requirements.
- Drug Testing and Financial Disclosure
- Security clearance: must be able to obtain and retain a "Q" security clearance with Special Compartmented Information (SCI) access.
- Must successfully complete a CI Evaluation, which may also include a CI-scope polygraph examination.

BENEFITS:

We offer a broad array of benefits. You may review our benefits and other helpful information by clicking [here](#).

Thank you for your interest in the U.S. Department of Energy's Office of Intelligence and Counterintelligence.

DIRECTIVES, GUIDANCE, AND DELEGATIONS

Directives

All current and archived Directives



Guidance

All current and archived DOE Guides



Delegations

Legal documents used to transfer authorities granted to the Secretary of Energy



NEWS & UPDATES

[Top 10](#)

[All Recently Issued/Updated Documents](#)

[Recently Canceled Directives](#)

[Recently Rescinded Delegations](#)

[Directives Quarterly Updates](#)

[Email Alerts](#)

[Technical Standards Portal](#)

[NSA Directives Portal](#)

New - DOE O 483.1B Chg 1 (MinChg), DOE Cooperative Research and Development Agreements

New - DOE O 442.1B, Department of Energy Employee Concerns Program

Draft - DOE G 424.1-1C, Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements

[More news...](#)

The Directives Program, Office of Management (MA-1.2) has collected Organizations' Assignment of Responsibility that derived from Directives and from the organization's responsible functional areas. In an effort to centralize this collection, they have been posted on the Directives, Guidance, and Delegations website at Organizations Assignments of Responsibility. Those associated with a directive(s) can also be found included with the directive in the "Related Content" section.



RevCom



Directives Tools



References



Delegation Procedures



Archives



Help

U.S. Department of Energy

Washington, D.C.

ORDER

DOE 5670.1A

01-15-92

SUBJECT: MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE

1. PURPOSE. To provide for the management of, and assign responsibilities for, the foreign intelligence activities of the Department of Energy (DOE). Foreign intelligence information is National Security Information (NSI) relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons that would impact United States national security or foreign relations.
2. CANCELLATION. DOE 5670.1, MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE, of 8-22-86.
3. REFERENCES.
 - a. Executive Order 12333, "United States (U.S.) Intelligence Activities," of 12-4-81, which provides for the organization and control of U.S. foreign intelligence activities.
 - b. Executive Order 12334, "President's Intelligence Oversight Board," of 12-4-81, which provides for oversight of intelligence activities to ensure their legality.

- b. Director of Intelligence (IN-1). As the Senior Intelligence Officer (SIO) for the Department and the Secretary's executive agent for implementing and monitoring the provisions of Executive Order 12333, as stated in paragraph 5a(2)(b) above, shall:
- (1) Manage the Department's foreign intelligence and counterintelligence programs.
 - (2) Manage the Department's intelligence organizations which shall:
 - (a) Prepare and coordinate the Department's foreign intelligence program budget, to include the DOE portion of the National Foreign Intelligence Program (NFIP), and submit appropriate DOE inputs to the Director of Central Intelligence (DCI), the Office of Management and Budget, and the Congress.
 - (b) Produce foreign political, economic, military, or facility threat-related intelligence and counterintelligence information responsive to requirements of Departmental Managers.
 - (c) Manage, coordinate, and oversee the production of foreign scientific and technical intelligence relating to nuclear proliferation, weapons, energy, threat-related, and emerging nuclear technologies in support of DOE and the Intelligence Community.
 - (d) Provide for DOE representation at DCI fora where matters and issues involving foreign intelligence and counterintelligence are concerned, including the National Foreign Intelligence Board (NFIB) and the National Foreign Intelligence Council (NFIC).
 - (e) Establish policies, plans, and procedures for the protection of all foreign intelligence and counterintelligence information in possession of DOE and its contractors.

U.S. DEPARTMENT OF ENERGY:
OFFICE OF
INSPECTOR GENERAL
HOTLINE

ighotline@hq.doe.gov

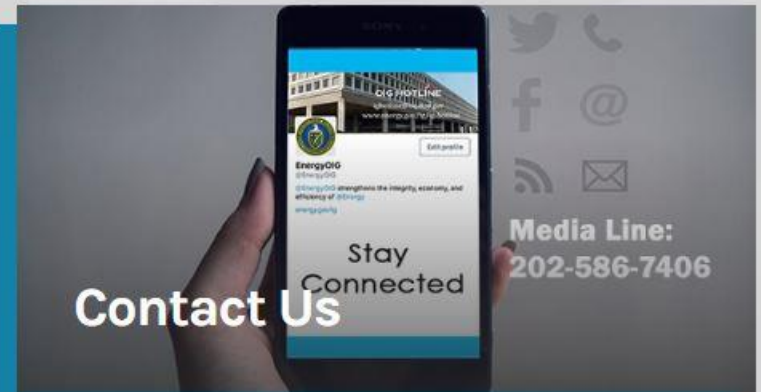
D.C. Metro Area: 202-586-4073

Toll free: (800) 541-1625

**Report Fraud, Waste, and
Abuse**



**Audit, Inspection, and
Other Reports**



Contact Us



**Media Line:
202-586-7406**

AUDIT, INSPECTION, AND EVALUATION RPTS. FROM 1995-PRESENT.

DATE: December 1, 1995

IN REPLY

REFER TO: IG-1

SUBJECT: INFORMATION: Report on Audit of the Department of Energy's Site Safeguards and Security Plans

TO: The Secretary

BACKGROUND:

The Department's Safeguards and Security program is designed to provide appropriate, efficient, and effective protection of the Department's nuclear weapons, nuclear materials, facilities, and classified information. Department of Energy policy, contained in DOE orders, specifies that Departmental interests shall be protected against a range of threats through the development of Site Safeguards and Security Plans (SSSPs). The SSSP is intended to depict the existing condition of safeguards and security site-wide and by facility, establish improvement priorities, and provide an estimate of the resources required to carry out the necessary improvements. The purpose of the audit was to determine if the Office of Safeguards and Security was using revised SSSP guidance as ldefacton policy to evaluate and approve SSSPs, and to determine if the new requirements established by the guidance were justified. The attached report is being sent to inform you of our findings and recommendations.

Improperly establishing policy is counter-productive to the Department's continuing efforts to meet Presidential initiatives to reduce regulatory requirements. In addition, the issuance of new guidance as ldefacton policy with unjustified increases for new SSSP requirements will cause the sites to spend millions of dollars for security improvements or compensatory measures.

Of the sites visited, three of the five locations had identified facilities that will be pushed above the Office of Safeguards and Security's acceptable level of low risk when the new security (consequence) values are incorporated. Each of the sites will need to devise and install additional compensatory measures to counter increases in the levels of risk caused by unjustified increases in consequence values.

The Savannah River Operations Office estimated it would need between \$5.1 million and \$6.7 million for security upgrades and enhancements along with an additional \$1.5 million to reevaluate their SSSPs. The Lawrence Livermore National Laboratory estimated it would spend almost \$100,000 annually to maintain additional protective force members. The Los Alamos National Laboratory estimated it would need about \$1.2 million annually to add protective force members and another \$400,000 for security system upgrades to compensate for the increase in risk. Cost estimates were not received from Rocky Flats Field Office and Idaho Operations Office. Rocky Flats could not provide a timely cost estimate and Idaho had already established security levels above the new requirements.

We recommend that the Director, Office of Nonproliferation and National Security ensure that the Office of Safeguards and Security coordinate all proposed policy changes and guidance, when used as policy, with affected program and field offices through the Departmental Directives System.

Management Comments. Management concurred in principle with the recommendations and stated that all proposed policy changes subject to the Directives System must be coordinated with program and field offices. It was further stated that guidance is not considered as policy and therefore implemented programs should not be subject to explicit inspection against the guidance. Requirements, whether or not justified, have never been and cannot be established by guidance. Within the Department, requirements can only be established by policy promulgated through the Directives System. Actual publication of policy, in the form of a Departmental directive is the last step in a process which involves coordination with organizations who are affected by the policy/requirement and who are in a position to provide meaningful input to the process. Guidance issued to the field is only intended as a means to share lessons learned in order to enhance the effectiveness and efficiency of site safeguards and security programs as they endeavor to meet requirements established in the directives.

Auditor Comments. Although management agreed in principle, their proposed actions do not meet the intent of the recommendation. As stated in our comments to

REVIEW OF ALLEGATIONS AGAINST A DEPARTMENT OF ENERGY'S OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE SENIOR OFFICIAL



Department of Energy
Washington, DC 20585

July 16, 2018

PURDUE
UNIVERSITY

Libraries

Finally, we did not substantiate the allegation that the senior official directed or influenced a contractor to hire his¹ relative. According to the senior official, his relative applied for the position and was subsequently offered the position. The senior official consulted with a General Counsel official prior to the contractor hiring the relative, and the General Counsel official advised that he (the senior official) should not be involved in the hiring process. Neither the General Counsel official nor the senior official was able to provide documentation of the conversation; however, the General Counsel official stated that although documentation of the conversation was not available, the General Counsel's office would have provided guidance to the senior official to not be involved in the hiring process in this type of situation. Further, the General Counsel official stated that based on the facts presented, there was not an appearance of improper influence, nor did the senior official need to recuse himself from his normal duties associated with contractor activities. Additionally, during our interviews with the contractor, the selecting official informed us that the relative was qualified, and stated that the senior official was not involved in the hiring process and did not influence the decision on the selection.

The allegations were not substantiated. As such, we have no recommendations or suggested

DEPARTMENT OF HOMELAND SECURITY

- National Cybersecurity and Communications Integration Center-Computer Emergency Response Team (CERT)
- Fusion Centers
- IG Reports

The National Cybersecurity and Communications Integration Center (NCCIC) is the Nation's flagship cyber defense, incident response, and operational integration center. Our mission is to reduce the Nation's risk of systemic cybersecurity and communications challenges.

Security alerts, tips, and other updates

ICS-CERT Alerts

An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

[change view]: [Alerts by Vendor](#)



- [ICS-ALERT-18-011-01 : Meltdown and Spectre Vulnerabilities \(Update J\)](#)
- [ICS-ALERT-17-341-01 : WAGO PFC200](#)
- [ICS-ALERT-17-216-01 : Eaton ELCSOFT Vulnerabilities](#)
- [ICS-ALERT-17-209-01 : CAN Bus Standard Vulnerability](#)
- [ICS-ALERT-17-206-01 : CRASHOVERRIDE Malware](#)
- [ICS-ALERT-17-181-01C : Petya Malware Variant \(Update C\)](#)
- [ICS-ALERT-17-135-01I : Indicators Associated With WannaCry Ransomware \(Update I\)](#)
- [ICS-ALERT-17-102-01A : BrickerBot Permanent Denial-of-Service Attack \(Update A\)](#)
- [ICS-ALERT-17-089-01 : Miele Professional PG 8528 Vulnerability](#)
- [ICS-ALERT-17-073-01A : MEMS Accelerometer Hardware Design Flaws \(Update A\)](#)
- [ICS-ALERT-16-286-01 : Sierra Wireless Mitigations Against Mirai Malware](#)
- [ICS-ALERT-16-263-01 : BINOM3 Electric Power Quality Meter Vulnerabilities](#)
- [ICS-ALERT-16-256-01 : FENIKS PRO Elnet Energy Meter Vulnerabilities](#)
- [ICS-ALERT-16-256-02 : Schneider Electric ION Power Meter CSRF Vulnerability](#)
- [IR-ALERT-L-16-230-01 : Navis WebAccess SQL Injection Exploitation](#)
- [ICS-ALERT-16-230-01 : Navis WebAccess SQL Injection Vulnerability](#)
- [ICS-ALERT-16-182-01 : Sierra Wireless AirLink Raven XE and XT Gateway Vulnerabilities](#)
- [ICS-ALERT-16-099-01B : Moxa NPort Device Vulnerabilities \(Update B\)](#)
- [IR-ALERT-H-16-056-01 : Cyber-Attack Against Ukrainian Critical Infrastructure](#)

1. EXECUTIVE SUMMARY

This updated alert is a follow-up to the updated alert titled ICS-ALERT-18-011-01 Meltdown and Spectre Vulnerabilities (Update I) that was published September 11, 2018, on the NCCIC/ICS-CERT website.

NCCIC is referencing CERT/CC's vulnerability note [VU#584653 CPU hardware vulnerable to side-channel attacks](#) to enhance the awareness of critical infrastructure asset owners/operators and to identify affected product vendors that have contacted ICS-CERT for help disseminating customer notifications/recommendations to mitigate the risk associated with cache side-channel attacks known as Meltdown and Spectre. Exploitation of these vulnerabilities may allow unauthorized disclosure of information.

[CVE-2017-5753](#), [CVE-2017-5715](#), and [CVE-2017-5754](#) have been assigned to these vulnerabilities.

The following product vendors have reported that they support products that use affected CPUs and have issued customer notifications with recommendations for users (NCCIC will update the list of vendors that have released customer notifications as additional information becomes available):

Please report any issues affecting control systems in critical infrastructure environments to NCCIC.

For details, please see each company's announcement:

- ABB: <http://search-ext.abb.com/library/Download.aspx?DocumentID=9AKK107045A8219&LanguageCode=en&DocumentPartId=&Action=Launch>
- Abbott: <http://www.abbott.com/policies/product-security-update.html>
- Beckman Coulter: <https://www.beckmancoulter.com/wsrportal/wsr/support/WannaCry-Ransomware-Cyber-attack/index.htm>
- Becton, Dickinson and Company (BD): www.BD.com/productsecurity
- Dräger: <https://static.draeger.com/security>
- Emerson (account required for login): <https://guardian.emersonprocess.com/Guardian/Components/ArticleViewer?type=KBA&articleId=9f769bec-d630-4cb7-9d06-fcc338c470e1>
- General Electric (account required for login, reference ID 000020832): <https://digitalsupport.ge.com>
- Honeywell: <https://www.honeywellprocess.com/en-US/support/Pages/security-updates.aspx>
- Johnson and Johnson: <http://www.productsecurity.jnj.com/advisories.html>



ICS-CERT Annual Assessment Report

Industrial Control Systems Cyber Emergency Response Team

FY 2016

PURDUE
UNIVERSITY

Libraries

2. FY 2016 Assessment Summary

We conducted 130 assessments in FY 2016, more than in any previous year. We also began a multi-year initiative to expand the number of Assessment teams we can field and to provide dedicated teams to support our Federal Government and CI customers, respectively. Figure 1 provides a quick snapshot of our FY 2016 activities.


FY 2016 Assessment Snapshot


ICS-CERT conducted **130 assessments** in FY 2016, including:



We identified **700 discoveries** through DAR and NAVV assessments.



 Boundary protection was the most commonly identified area of weakness from FY 2014–FY 2016.

 Weaknesses related to boundary protection represented 13.4 percent of all discovered weaknesses.



The *Energy, Government Facilities, Transportation Systems, and Water and Wastewater Systems Sectors* were the most frequently assessed critical infrastructure sectors, together representing 75 percent of all assessments.

State & Major Urban Area Fusion Centers

Building Law Enforcement and DHS Partnerships

Coordinating Federal Support for Fusion Centers

Deployed Intelligence Officers and Protective Security Advisors

Fact Sheet

Fusion Center Foundational Guidance

Fusion Center Performance Program

Fusion Centers Handout

Locations and Contact Information

P/CRCL for Fusion Centers

Resources for Fusion Centers

Success Stories

Support of National Strategies and Guidance

State and Major Urban Area Fusion Centers

Fusion centers operate as state and major urban area focal points for the receipt, analysis, gathering, and sharing of threat-related information between federal; state, local, tribal, territorial (SLTT); and private sector partners.

[Expand All Sections](#)

Fusion Center Value +

DHS's Partnership with the National Network +

Learn More +

Fusion Center Value

The National Network of Fusion Centers (National Network) brings critical context and value to homeland security and law enforcement that no other federal or local organization can replicate. Fusion centers accomplish this through their:

Unique Information

Fusion centers are information sharing hubs that provide comprehensive and [appropriate access](#), analysis, and dissemination that no other single partner can offer.

Unique Perspective

Independence from federal partners allows fusion centers to provide [partners](#) with a unique perspective on threats to their state or locality, contributing to the national threat picture.

Unique Role

Homeland Security Grant Program (HSGP)

The FY 2018 Homeland Security Grant Program (HSGP) plays an important role in the implementation of the National Preparedness System (NPS) by supporting the building, sustainment, and delivery of core capabilities essential to achieving the National Preparedness Goal (NPG) of a secure and resilient Nation. Delivering core capabilities requires the combined effort of the whole community, rather than the exclusive effort of any single organization or level of government. The FY 2018 HSGP's allowable costs support efforts to build and sustain core capabilities across the [Prevention](#), Protection, Mitigation, Response, and Recovery mission areas, including the following priorities:

- Building and Sustaining Law Enforcement Terrorism Prevention Capabilities
- Maturation and Enhancement of State and Major Urban Area Fusion Centers

DHS preparedness grants continue to prioritize support for [designated State and major Urban Area fusion centers](#) and the maturation of the Information Sharing Environment (ISE). Fusion centers, a critical component of our Nation's distributed homeland security and counterterrorism architecture, provide grassroots intelligence and analytic capabilities within the state and local environment.

In support of this strategic vision and as a requirement of the HSGP, the Department of Homeland Security, Office of Intelligence and Analysis (I&A) requires designated State and major urban area fusion centers to participate in an [annual assessment](#) of their performance.

Furthermore, as a requirement of the HSGP, DHS requires that all fusion center related funding requests be consolidated into a single (1) Investment for States or Urban Areas in which designated fusion centers reside, and this Investment must address funding support for the designated fusion center. The single Investment provides state and urban areas a means to centrally manage and report on fusion center related activities. Grantees must coordinate with the fusion center when developing a fusion center Investment prior to submission. The fusion center must utilize its individual assessment data



IIFC

Contact Us

Mission & Vision

Privacy Policies

Statute

Indiana Crime Information Network

Missing Children/Missing Endangered Adults

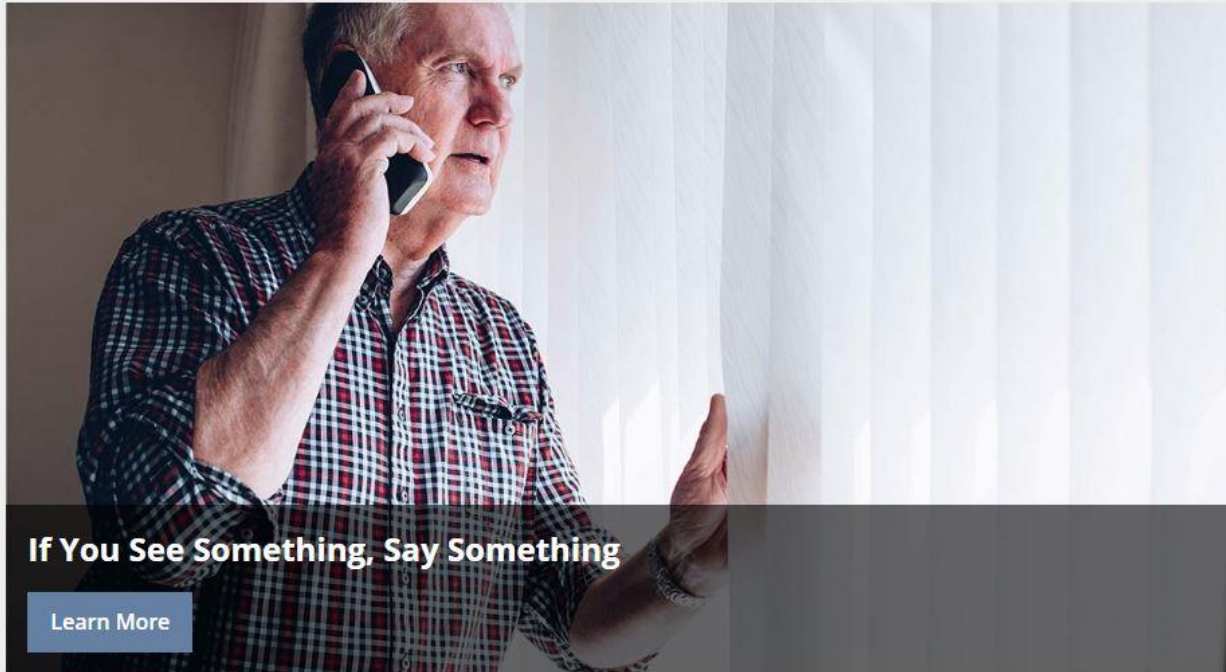
Resources

"IF YOU SEE SOMETHING, SAY SOMETHING!"

8 Signs of Terrorism

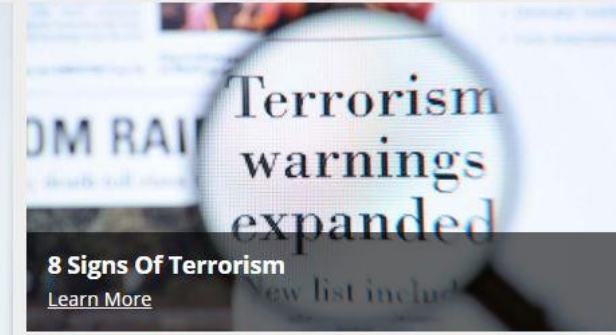
Project LENS

Indiana State Police



If You See Something, Say Something

Learn More



8 Signs Of Terrorism

Learn More



Report Suspicious Activity

Learn More

Welcome

The mission of the Indiana Intelligence Fusion Center is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal and terrorist activity in the State of Indiana while following Fair Information Practices to ensure the rights and privacy of citizens.

Mission

FOIA/Privacy Act Office

Partner Engagement

State & Major Urban Area Fusion Centers

Office of Intelligence and Analysis Mission

The mission of the Intelligence and Analysis (I&A) is to equip the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient. I&A's vision is a premier Homeland Security Intelligence Enterprise, driving information sharing and delivering unique predictive intelligence and analysis to operators and decision-makers at all levels.

The Office of Intelligence and Analysis (I&A) is the only element of the [U.S. Intelligence Community](#) statutorily charged with delivering intelligence to our state, local, tribal, territorial and private sector partners, and developing intelligence from those partners for the Department and the IC.

Information Sharing

I&A serves as the information conduit and intelligence advocate for state, local, tribal, and territorial governments. I&A supports the National Network of Fusion Centers (National Network) with deployed personnel and systems, training, and collaboration. The National Network is the hub of much of the two-way intelligence and information flow between the federal government and our state, local, tribal and territorial partners. The fusion centers represent a shared commitment between the federal government and the state and local governments who own and operate them. Individually, each is a vital resource for integrating information from national and local sources to prevent and respond to all threats and hazards. Collectively, their collaboration with the federal government, one another (state-to-state and state-to-locality), and with the private sector represents the new standard through which we view homeland security. [Fusion centers have contributed](#) and will continue to contribute to improvements in information sharing and collaboration that will enhance the nation's overall preparedness.

I&A assumes the program management role for the Department's engagement with the [Nationwide Suspicious Activity Reporting \(SAR\) Initiative \(NSI\) Program Management Office \(PMO\)](#). As part of that role, I&A is a direct liaison with the NSI PMO and facilitates the efforts of DHS components and fusion centers in becoming active NSI participants. Additionally, I&A leverages SAR data to create analytical products that assist federal, state, local and tribal partners in their respective homeland security missions.





NATIONWIDE SAR INITIATIVE (NSI)



Home

About the NSI

Items of Interest

NSI Partners

NSI Participation Map

Online SAR Training

On-Site SAR Training

Resources

Outreach Resources

Report Line Officer Training



"Whether a plan for a terrorist attack is homegrown or originates overseas, important knowledge that may forewarn of a future attack may be derived from information gathered by State, local, and tribal government personnel in the course of routine law enforcement and other activities."

—National Strategy for Information Sharing, October 2007

The Nationwide SAR Initiative

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a joint collaborative effort by the U.S. Department of Homeland Security, the Federal Bureau of Investigation, and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.

The NSI is a standardized process—including stakeholder outreach, privacy protections, training, and facilitation of technology—for identifying and reporting suspicious activity in jurisdictions across the country and also serves as the unified focal point for sharing SAR information.

[Read more about the NSI](#)

[Access NSI Documents and Resources](#)

Announcement:

- Release of [Information Sharing Environment \(ISE\) Functional Standard \(FS\) Suspicious Activity Reporting \(SAR\) 1.5.5](#)



FINAL REPORT:
INFORMATION SHARING ENVIRONMENT
(ISE)-SUSPICIOUS ACTIVITY REPORTING (SAR)

EVALUATION
ENVIRONMENT

METHODOLOGY TO MEASURE, DOCUMENT, AND EVALUATE THE ISE-SAR EE

The ISE-SAR EE was developed to test the assumptions of sharing ISE-SAR information across multiple domains in accordance with the ISE-SAR Functional Standard and business rules. The project sought to identify pilot site partners from state and major urban area fusion centers, DOJ, and DHS. The ISE-SAR EE examined the usefulness of the ISE-SAR Criteria Guidance (Part B of the ISE-SAR Functional Standard) and the sharing of ISE-SAR information among major city and other law enforcement agencies, JTTFs, and fusion centers. The Evaluation Environment has provided the capability to establish, test, and validate the end-to-end agency SAR processes, including the development of priority information needs, information gathering and reporting policies, report vetting and analysis, and other enabling activities.

Following meetings with the participating agencies, the project partners developed an assessment for each of the pilot sites to evaluate their current SAR processes and procedures and to determine the standing and threat-based information sharing need priorities. Additionally, the site visits were conducted to evaluate the existing technology capabilities and current business processes surrounding the gathering, analysis, and sharing of terrorism-related SAR information. These site visits allowed project partners to document the “As-Is” SAR process of the pilot sites. The discussion and determination of



HIGHLIGHTS

Fiscal Year 2016 Evaluation of DHS' Compliance with Federal Information Security Modernization Act Requirements for Intelligence Systems

Unclassified Summary

May 9, 2017

We reviewed the Department of Homeland Security's (DHS) information security program for intelligence systems in accordance with requirement of the *Federal Information Security Modernization Act*. The objective of our review was to determine whether DHS' information security program and practices are adequate and effective in protecting the information and information systems supporting DHS' intelligence operations and assets. We assessed DHS programs for continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, plans of action and milestones, remote access management, contingency planning, and contractor

GENERA

Office of Intelligence and Analysis Can Improve Transparency and Privacy

Why We Did This Audit

We evaluated the Office of Intelligence and Analysis' (I&A) safeguards for the sensitive privacy and intelligence information it collects and maintains. Our objective was to determine whether I&A ensures compliance with Federal laws, regulations, and policies.

What We Recommend

We are making six

Specifically, I&A has centralized the oversight of privacy and civil liberties and has been working to ensure that it meets the requirements of pertinent legislation, regulations, directives, and guidance. I&A conducted specialized onboarding and advanced training that address safeguards for privacy and civil liberties in its intelligence processes. In addition, I&A designed intelligence oversight reviews to ensure that its employees observe the required safeguards.

However, I&A has faced challenges because it did not place priority on institutionalizing other capabilities and processes to ensure timely and complete compliance with requirements regarding privacy and intelligence information. Specifically:

- I&A has not responded timely to requests for agency transparency under the *Freedom of Information Act*, potentially creating financial liabilities.
- I&A continuity capabilities have not had an adequate oversight structure, risking the loss of essential records and intelligence information in an emergency.
- I&A has not implemented an infrastructure for risk assessment and end-to-end monitoring of high-impact solicitations and contracts that would ensure safeguards for sensitive data and systems throughout the acquisition processes.

Recommendations

We recommend that the Principal Deputy Under Secretary for Intelligence and Analysis:

Recommendation 1: Prepare a plan of action and milestones for providing the FOIA Office appropriate staffing and capabilities to reduce its backlog of unresolved requests.

Recommendation 2: Provide specialized training for FOIA staff, Division contacts, and operational staff to improve I&A's responsiveness to FOIA requests.

Recommendation 3: Prepare a plan of action and milestones for instituting an organization-wide records management structure and processes to improve timeliness in identifying and locating pertinent records to address FOIA requests.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Under Secretary for Intelligence and Analysis. Management concurred with our recommendations. We have included a copy of the comments in their entirety in appendix B. The planned corrective actions and milestones satisfy the intent of these recommendations. We look forward to receiving updates on the implementation progress.

Bureau of Intelligence and Research

INR is a bureau of the Department of State and a member of the **Intelligence Community** (IC). The Bureau of Intelligence and Research's (INR) primary mission is to harness intelligence to serve U.S. diplomacy. Secretary of State George Marshall established INR in 1947. INR is a direct descendant of the Office of Strategic Services Research Department and the oldest civilian intelligence element in the U.S. Government. **Ellen E. McCarthy** is INR's Assistant Secretary.

Drawing on all-source intelligence, INR provides value-added independent analysis of events to U.S. State Department policymakers; ensures that intelligence activities support foreign policy and national security purposes; and serves as the focal point in the State Department for ensuring policy review of sensitive counterintelligence and law enforcement activities around the world. The bureau directs the Department's program of intelligence analysis and research, conducts liaison with the Intelligence Community, and represents the Department on committees and in interagency intelligence groups. The Bureau of Intelligence and Research also analyzes geographical and international boundary issues.

BUREAU OF INTELLIGENCE AND RESEARCH

- Achieves mission objectives via:
- All-Source Analysis: Focuses on supporting diplomats & diplomacy with multiple information and analyses ranges. Drafts President's Daily Brief and is U.S. Govt. leader for foreign public opinion research.
- Intelligence Policy & Coordination: Coordinates between State Dept. and Intelligence Community to ensure intelligence collection and operations support and inform foreign policy. Conducts policy review of sensitive intelligence, counterintelligence, and law enforcement within State Dept. to ensure consistency with foreign policy interests.
- Analytic Outreach: Provides analysts and policymakers with perspectives from the private sector, academe, and non-governmental experts on the most challenging foreign policy and

ADDITIONAL INTELLIGENCE AND RESEARCH ENTITIES

- INR Front Offices & Components
- Analytic Support & Production Staff
- Analytic Offices
- Office of Analysis for African Affairs
- Office of Analysis for East Asia & the Pacific
- Office of Economic Analysis
- Office of the Geographer & Global Issues
- Office of Opinion Research
- Office of Analysis for Russia and Eurasia
- Office of Strategic, Proliferation, & Military Issues
- Intelligence & Policy Coordination
- Office of Consular & Management Liaison
- Office of Cyber Affairs
- Office of Intelligence Operations & Oversight
- Office of Intelligence Policy & Information Sharing Center
- Office of Technical Collection Affairs

Independent States in the World

Fact Sheet

BUREAU OF INTELLIGENCE AND RESEARCH

Washington, DC

February 15, 2019

See also:

[Dependencies and Areas of Special Sovereignty](#)

Total count of independent states: 195

* Diplomatic relations with the United States

+ Member of United Nations

! New change, since previous list

STATE

Short-form name	Long-form name	GENC 2A Code (see Note 2)	GENC 3A Code (see Note 2)	Capital
Afghanistan *+	Islamic Republic of Afghanistan	AF	AFG	Kabul
Albania *+	Republic of Albania	AL	ALB	Tirana

Dependencies and Areas of Special Sovereignty

Fact Sheet

BUREAU OF INTELLIGENCE AND RESEARCH

Washington, DC

March 7, 2017

See also:

[Independent States in the World](#)

! New change, since previous list

Short-form name	Long-form name	Sovereignty	!GENC 2A Code (see note 1)	!GENC 3A Code (see note 1)	Administrative Center
Akrotiri (see note 15)	Akrotiri	United Kingdom	QZ	XQZ	Episkopi (see note 16)
American Samoa	Territory of American Samoa	United States	AS	ASM	Pago Pago
Anguilla	Anguilla	United Kingdom	AI	AIA	The Valley
Antarctica	(no long-form name)	None (see note 2)	AQ	ATA	None
Aruba	Aruba	Netherlands	AW	ABW	Oranjestad

Report to Congress per P.L. 110-286 on Military and Intelligence Aid to Burma for 2011



Released September 16, 2013

Under Section 10 of Public Law 110-286, the Secretary of State is required to submit to the Committee on Foreign Affairs of the House of Representatives and the Committee on Foreign Relations of the Senate "a report containing a list of countries, companies, and other entities that provide military or intelligence aid to the SPDC and describing such military or intelligence aid provided by each country, company or other entity."

Overview

In 2011, Burma's primary foreign suppliers of weapons and military-related technology were state-controlled arms companies from China, North Korea, Russia, and Belarus. Intelligence aid, if any, will be included in the classified annex.

Assistance by Country

China and Chinese companies provided both finished military equipment and military production assistance to Burma.

North Korea and North Korean companies supported Burma's efforts to build and operate military-related production facilities. North Korea's arms traders bought production-related equipment for work in Burma from companies based in Taiwan and China.

Russian companies or brokers continued to deliver aircraft to Burma in 2011. Russia also continued to train Burmese students in a wide range of fields with military applications.

Belarus' state-owned supply company delivered helicopters and related equipment.

Firms based in **Singapore, Taiwan, and Thailand** have reportedly assisted Burma's defense industry in acquiring production technology.

Sudan: Death Toll in Darfur

It is estimated that 98-181,000 people have died since March 2003 in the conflict-affected area of Darfur and eastern Chad. Excluding an expected "normal" base mortality total of 35,000 deaths for this population, 63-146,000 "excess" deaths can be attributed to violence, disease, and malnutrition because of the conflict. Wildly divergent death toll statistics, ranging from 70,000 to 400,000, result from applying partial data to larger, nonrepresentative populations over incompatible time periods. Violent deaths were widespread in the early stages of this conflict, but a successful, albeit delayed, humanitarian response and a moderate 2004 rainy season combined to suppress mortality rates by curtailing infectious disease outbreaks and substantial disruption of aid deliveries.

Estimating Mortality: Rationale and Methodology

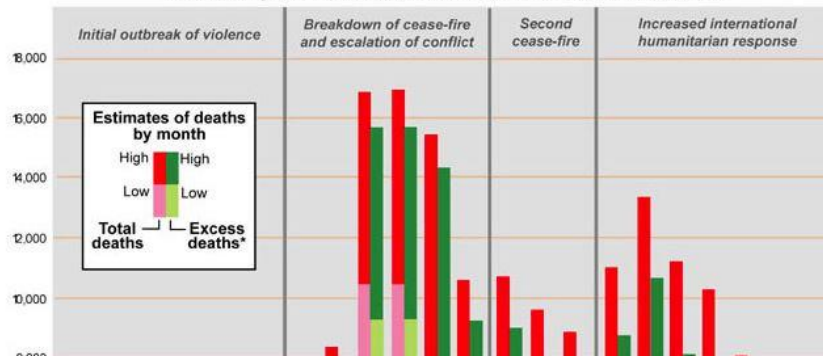
Insufficient data are available to determine Darfur's death toll, a number that will probably never be fully known. The most important factor distorting the debate on deaths in Darfur has been the application of elevated mortality rates derived from site-specific surveys of displaced populations to the broader affected populace, of which they are not representative.

Many extrapolations do not factor in the progression and intensity of the conflict in different areas of Darfur and the consequent shift in rates over time and region. The misconception that violence, not infectious disease outbreaks, is the primary cause of death in most populations affected by conflict also has skewed the many projections regarding loss of life.

The following analysis draws on available information—epidemiological surveys, displacement trends, and patterns of village destruction—to estimate the progression of the conflict and associated mortality rates throughout the three Darfur states from March 2003 to early 2005. Mortality rates were ascertained first from a compilation of more than 30 health and mortality studies conducted in the region; these were applied to other populations experiencing similar levels of violence and displacement to derive mortality estimates for affected populations by state and month. "High" and "low" estimates of mortality rates were then applied to UN data for all affected populations. Separate rates were applied to displaced and otherwise affected populations with different levels of vulnerability.

Total Deaths and Excess Deaths* in Darfur and the Chad Refugee Camps High and Low Estimates, March 2003 - January 2005

* Deaths owing to violence, disease, and malnutrition attributable to the conflict.



378a

DEPARTMENT OF STATE
BUREAU OF INTELLIGENCE AND RESEARCH

Research Memorandum
RFE-14, January 10, 1962

SUMMARY OF PRINCIPAL EVENTS IN THE HISTORY OF VIETNAM¹

This Research Memorandum is designed to present in brief narrative form the principal events in the history of Vietnam, particularly since 1945. It lists events decisive in themselves or in Vietnam's evolution to the status of an independent state and indicative of the serious problems the country has faced since independence. While not purporting to be complete or exhaustive, it up-dates and expands considerably an earlier report, IR-6048, Summary of Significant Events in the Histories of Vietnam, Cambodia, and Laos, October 24, 1952. The classification of this report, as in the case of the earlier one, is intended to facilitate wide distribution.

Year (A.D.)

939 Vietnamese achieve independence after one thousand years of Chinese domination.

DEPARTMENT OF STATE
BUREAU OF INTELLIGENCE AND RESEARCH

Research Memorandum
RES-19, July 8, 1963

TO : The Secretary
THROUGH: S/S
FROM : INR - Thomas L. Hughes *Thomas L. Hughes*
SUBJECT: Shortcomings in Soviet Transportation, [R. ...]

Soviet speeches and publications provide a considerable amount of information on the problems besetting the transportation industry despite its rapid strides in recent years. This report discusses the major transportation deficiencies of the USSR as seen through Soviet eyes during the period 1961-63.

ABSTRACT

The volume of traffic handled by Soviet freight carriers is about equal to that of the US but from an economic and technical viewpoint performance falls far short of Western standards. Government programs call for a major shift from the high cost, over-burdened railroads which now handle about four-fifths of all traffic.

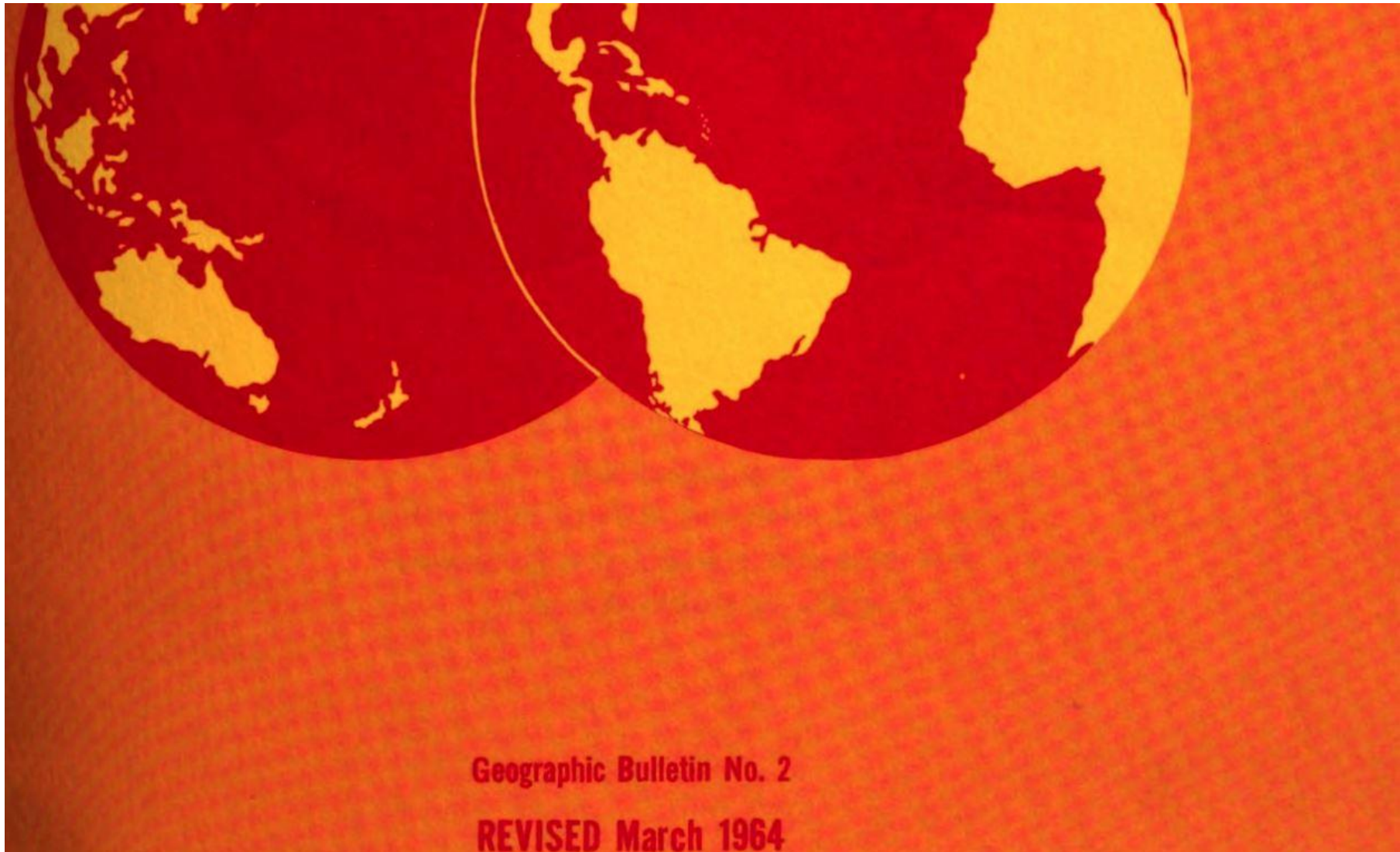
I.	Introduction	4
II.	General Deficiencies	4
III.	Rail Transportation	9
	A. Productivity and Innovation	9
	B. Construction of New Lines	9
	C. Laying of Track, Ties and Rails	10
	D. Locomotives and Rolling Stock	12
	E. Organization and Coordination	14
	F. Crosshauls and Comfort	15
IV.	Highway Transportation	16
V.	Inland Waterway Navigation	17
VI.	Maritime and Caspian Sea Transportation	21
VII.	Civil Aviation	27
VIII.	Pipelines	29

Table 2. USSR TRANSPORT PERFORMANCE, BY TYPE OF TRANSPORTATION, 1961 AND 1962

(in billions of metric ton-kilometers)

Type	Year				Increase (in percent)
	1961		1962		
	Amount	Percent	Amount	Percent	
Rail	1,566	78.4	1,646	77.7	5.1
Motor	106	5.3	113	5.3	6.6
Inland waterways	106	5.3	110	5.2	3.8
Sea	159	8.0	173	8.2	8.8
Pipelines (oil)	60	3.0	75	3.6	25.0
Airways	1	<u>insig</u>	1	<u>insig</u>	<u>insig</u>
Total	1,998	100.0	2,118	100.0	6.0

SOURCE: Official Soviet statistics.



Geographic Bulletin No. 2

REVISED March 1964

PURDUE
UNIVERSITY

Libraries

Status of the World's Nations

A BRIEF SURVEY

The year 1964 started with 122 states in the world generally accepted as independent.¹ This number has increased sharply during recent decades: On the eve of World War I, 53 countries were independent (as their status would be evaluated by current criteria); on the eve of World War II, 71 countries were independent.

A fast-changing international situation following each of the world wars fostered the creation of new sovereign states without equating dissolution of existing ones. In fact, from 1914 to 1963 surprisingly few of the world's sovereign states disappeared

the Soviet Union.² Other states disappeared temporarily from the world community during the war, including Austria, Czechoslovakia, and Ethiopia.

Finally, as an exceptional situation, Syria in 1958 joined Egypt to constitute a part of the United Arab Republic for 3 years. During that time it did not retain its identity as a separate state. Two somewhat similar situations came under consideration during 1963, although in neither case did an actual change in sovereign status materialize: (1) the United Arab Republic and other Arab States sought for a time to

IRREGULAR CATEGORIES OF POLITICAL AREAS AND REGIMES

Several political areas and regimes acknowledged as such by the U.S. Government defy classification because of a particular status or by virtue of the tradition and historical sequence through which they evolved. Despite their special status these areas frequently appear on maps along with other political entities, at times without distinction by style of type. The more important of them are briefly identified in the following paragraphs.

Palestine

The boundaries of Israel have never been definitely established, with the result that Palestine occasionally has been listed separately. On April 24, 1950, Jordan announced the annexation of that portion of Palestine remaining under Jordanian control after the general Armistice Agree-

divided between the two countries controlling it jointly. Another neutral zone—a small fraction of a square mile—lies between Spanish and British territory (Gibraltar) in the extreme southern part of the Iberian Peninsula.

Outer Mongolia

Outer Mongolia, a geographic term, generally corresponds in area to the "Mongolian People's Republic." Although admitted as a member by the United Nations on October 27, 1961, Outer Mongolia has not been recognized by the Government of the United States.

Tibet

The United States has regarded Tibet historically as being autonomous under Chinese suzerainty.

The West Indies Federation

TREASURY DEPT. INTELLIGENCE

- Office of Intelligence and Analysis-Terrorism & Financial Intelligence
 - Missions:
 - Driving intelligence to meet Treasury decision-makers and external customers.
 - Producing all-source assessments & other materials to identify threats and vulnerabilities in licit and illicit networks which may be addressed by Treasury Dept. action.
 - Delivering timely, accurate, and relevant intelligence to decision-makers.
 - Providing necessary security infrastructure to safeguard the Treasury's national security information.
- Key Activities:
 - Safeguarding financial system against illicit use, combating rogue nations, terrorist facilitators, weapons of mass destruction proliferators, money launderers, drug kingpins, and other national security threats.
 - Tools:
 - Office of Foreign Assets Control (OFAC) lists Specially Designated Nationals (SDNs) and enforces other economic sanctions against individuals, nations, and organizations.

TREASURY DEPT. INTELLIGENCE TOOLS

- Section 311 of USA Patriot Act gives Treasury Secretary options to effectively target specific terrorist financing risks and money laundering and protect U.S. financial system from specific threats.
- Asset Forfeiture: Effective law enforcement actions against criminal enterprises, from drug cartels to terrorist organizations, requires depriving them of their enabling assets and profits that support or stem from their existence. The Treasury Forfeiture Fund (TFF) is derived from the forfeited assets of criminal enterprises.
- Financial Action Task Force (FATF) International policymaking and standard setting body dedicated to combating international money laundering and terrorist financing



OFFICE OF FOREIGN ASSETS CONTROL

Specially Designated Nationals and Blocked Persons List

February 25, 2019

ALPHABETICAL LISTING OF SPECIALLY DESIGNATED NATIONALS AND BLOC KED PERSONS ("SDN List"):

This publication of Treasury's Office of Foreign Assets Control ("OFAC") is designed as a reference tool providing actual notice of actions by OFAC with respect to Specially Designated Nationals and other persons (which term includes both individuals and entities) whose property is blocked, to assist the public in complying with the various sanctions programs administered by OFAC. The latest changes to the SDN List may appear here prior to their publication in the Federal Register, and it is intended that users rely on changes indicated in this document. Such changes reflect official actions of OFAC, and will be reflected as soon as practicable in the Federal Register under the index heading

a.k.a. 7TH OF TIR INDUSTRIES; a.k.a. 7TH OF TIR INDUSTRIES OF ISFAHAN/ESFAHAN; a.k.a. MOJTAMAE SANATE HAFTOME TIR; a.k.a. SANAYE HAFTOME TIR; a.k.a. SEVENTH OF TIR), Mobarakeh Road Km 45, Isfahan, Iran; P.O. Box 81465-478, Isfahan, Iran; Additional Sanctions Information - Subject to Secondary Sanctions [NPWMD] [IFSR].

7TH OF TIR COMPLEX (a.k.a. 7TH OF TIR; a.k.a. 7TH OF TIR INDUSTRIAL COMPLEX; a.k.a. 7TH OF TIR INDUSTRIES; a.k.a. 7TH OF TIR INDUSTRIES OF ISFAHAN/ESFAHAN; a.k.a. MOJTAMAE SANATE HAFTOME TIR; a.k.a. SANAYE HAFTOME TIR; a.k.a. SEVENTH OF TIR), Mobarakeh Road Km 45, Isfahan, Iran; P.O. Box 81465-478, Isfahan, Iran; Additional Sanctions Information - Subject to Secondary Sanctions [NPWMD] [IFSR].

7TH OF TIR INDUSTRIAL COMPLEX (a.k.a.

8TH IMAM INDUSTRIES GROUP (a.k.a. CRUISE MISSILE INDUSTRY GROUP; a.k.a. CRUISE SYSTEMS INDUSTRY GROUP; a.k.a. NAVAL DEFENCE MISSILE INDUSTRY GROUP; a.k.a. SAMEN AL-A'EMMEH INDUSTRIES GROUP), Tehran, Iran; Additional Sanctions Information - Subject to Secondary Sanctions [NPWMD] [IFSR].

32 COUNTY SOVEREIGNTY COMMITTEE (a.k.a. 32 COUNTY SOVEREIGNTY MOVEMENT; a.k.a. IRISH REPUBLICAN PRISONERS WELFARE ASSOCIATION; a.k.a. REAL IRA; a.k.a. REAL IRISH REPUBLICAN ARMY; a.k.a. REAL OGLAIGH NA HEIREANN; a.k.a. RIRA) [FTO] [SDGT].

32 COUNTY SOVEREIGNTY MOVEMENT (a.k.a. 32 COUNTY SOVEREIGNTY COMMITTEE; a.k.a. IRISH REPUBLICAN PRISONERS WELFARE ASSOCIATION; a.k.a.

NOTE: The SDNs are listed by country of residence or incorporation. There are, however, SDNs with no fixed residence or country of incorporation. These entities are listed at the end of the Country List under the heading of "Undetermined". It is advisable to check both the Country list and the Undetermined list when searching for an SDN.

Afghanistan

AAFIA SIDDIQUE BRIGADE (a.k.a. JAMAAT-E-AHRAR; a.k.a. JAMAATUL AHRAR; a.k.a. JAMAATUL-AHRAR; a.k.a. JAMAAT-UL-AHRAR; a.k.a. JAMAAT-UL-AHRAR TTP; a.k.a. JAMATUL AHRAR; a.k.a. JAMAT-UL-AHRAR; a.k.a. TEHREEK-I-TALIBAN JAMAAT-UL-AHRAR; a.k.a. TEHRIK-E-TALIBAN PAKISTAN JAMAAT-E-AHRAR; a.k.a. "JUA"; a.k.a. "TTP-JA"; a.k.a. "TTP-JUA"), Afghanistan; Mohmand Tribal Agency, Pakistan; Bajaur Tribal Agency, Pakistan; Khyber Tribal Agency, Pakistan; Arakzai Tribal Agency, Pakistan; Charsadda, Pakistan; Peshawar, Pakistan; Swat, Pakistan; Punjab Province, Pakistan [SDGT].

ABDULASATTAR (a.k.a. BARAKZAI, Haji Abdul Sattar; a.k.a. BARAKZAI, Haji Satar; a.k.a. MANAN, Haji Abdul Satar Haji Abdul; a.k.a. SATAR, Haji Abdul), Kachray Road, Pashtunabad, Quetta, Balochistan Province, Pakistan; Nasrullah Khan Chowk, Pashtunabad Area, Balochistan Province, Pakistan; Chaman, Balochistan Province, Pakistan; Abdul Satar Food Shop, Eno Mina 0093, Kandahar, Afghanistan; DOB 1964; POB Mirmandaw Village, Nahr-e Saraj District, Helmand Province, Afghanistan; alt. POB Qilla Abdullah, Pakistan; alt. POB Mirmadaw Village, Gereshk District, Helmand Province, Afghanistan; Passport AM5421691 (Pakistan) expires 11 Aug 2013; National ID No. 5420250161699 (Pakistan); alt. National ID No. 585629 (Afghanistan) (individual) [SDGT] (Linked To: HAJI KHAIRULLAH HAJI SATTAR MONEY EXCHANGE; Linked To: TALIBAN).

ABDULLAH, Abdullah Ahmed (a.k.a. AL-MASRI, Abu Mohamed; a.k.a. "ABU MARIAM"; a.k.a. "SALEH"), Afghanistan; DOB 1963; POB Egypt; citizen Egypt (individual) [SDGT].

ABDUREHMAN, Ahmed Mohammed (a.k.a. AHMED, Ahmed; a.k.a. ALI, Ahmed Mohammed; a.k.a. ALI, Ahmed Mohammed Hamed; a.k.a. ALI, Hamed; a.k.a. AL-MASRI, Ahmad; a.k.a. AL-SURIR, Abu Islam; a.k.a. HEMED, Ahmed; a.k.a. SHIEB, Ahmed; a.k.a. "ABU FATIMA"; a.k.a. "ABU ISLAM"; a.k.a. "ABU KHADIIJAH"; a.k.a. "AHMED HAMED"; a.k.a. "AHMED THE EGYPTIAN"; a.k.a. "SHUAIB"), Afghanistan; DOB 1965; POB Egypt; citizen Egypt (individual) [SDGT].

Venezuela-related Designations

2/25/2019

OFFICE OF FOREIGN ASSETS CONTROL

Specially Designated Nationals List Update:

The following individuals have been added to OFAC's SDN List:

CARRIZALEZ RENGIFO, Ramon Alonso (a.k.a. CARRIZALES, Ramon), Apure, Venezuela; DOB 08 Nov 1952; Gender Male; Cedula No. 2516238 (Venezuela) (individual) [VENEZUELA].

GARCIA CARNEIRO, Jorge Luis (a.k.a. GARCIA CARNEIRO, Jorge), La Guaira, Vargas, Venezuela; DOB 08 Feb 1952; POB Caracas, Venezuela; Gender Male; Cedula No. 4169273 (Venezuela) (individual) [VENEZUELA].

LACAVA EVANGELISTA, Rafael Alejandro (a.k.a. LACAVA EVANGELISTA, Rafael; a.k.a. LACAVA, Rafael), Carabobo, Venezuela; DOB 03 Sep 1968; Gender Male; Cedula No. 8611651 (Venezuela) (individual) [VENEZUELA].

PRIETO FERNANDEZ, Omar Jose (a.k.a. PRIETO, Omar), San Francisco, Zulia, Venezuela; DOB 25 May 1969; Gender Male; Cedula No. 9761075 (Venezuela) (individual) [VENEZUELA].





Civil Penalties and Enforcement Information

2019 Enforcement Information

Browse OFAC Enforcement Actions By Year

[2019](#) | [2018](#) | [2017](#) | [2016](#) | [2015](#) | [2014](#) | [2013](#) | [2012](#) | [2011](#) | [2010](#) | [2009](#) | [2008](#) | [2007](#) | [2006](#) | [2005](#) | [2004](#) | [2003](#)

Civil Penalties Information Chart

Detailed Penalties Information	Aggregate Number of Penalties or Settlements	Monthly Penalties/Settlements Total in USD
02/21/2019 	1	506,250
02/14/2019 	1	5,512,564
02/07/2019 	1	13,381
01/31/2019 	1	996,080
Year to date totals:	4	7,028,275

Additional Selected Settlement Agreements

- [Selected Settlement Agreements from 2019 to 2009](#)

Additional Guidance on OFAC's Enforcement and Compliance Policies


- [OFAC Enforcement Guidelines](#) 
- [Memoranda of Understanding Between OFAC and Bank Regulators](#)
- [Guidance on Submitting Electronic Documents to OFAC Enforcement](#)

Statutes, Rules and Regulations Relating to OFAC Settlements and Civil Penalties

Statutes

- [IEEPA, 50 USCS Sec 1701](#) 
- [TWEA, 50 USCS Sec 5](#) 

Code of Federal Regulations

- [31 CFR 501](#)  Reporting, Procedures, and Penalties Regulations

ENFORCEMENT INFORMATION FOR February 21, 2019

Information concerning the civil penalties process can be found in the Office of Foreign Assets Control (OFAC) regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. These references, as well as recent final civil penalties and enforcement information, can be found on OFAC's website at www.treasury.gov/ofac/enforcement.

ENTITIES – 31 CFR 501.805(d)(1)(i)

ZAG IP, LLC Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations: ZAG IP, LLC (formerly known as ZAG International, LLC) (“ZAG”), a U.S. company with its business address in Newtown, Connecticut, has agreed to pay \$506,250 to settle its potential civil liability for five apparent violations of § 560.206 of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560 (ITSR). Specifically, between on or about July 11, 2014 and on or about January 15, 2015, through five separate transactions, ZAG purchased a total of 263,563 metric tons of Iranian-origin clinker from a company located in the United Arab Emirates, with knowledge that the cement clinker was sourced from Iran, and then resold and transported it to a company in Tanzania. The aggregate value of the five transactions was \$14,495,961.

OFAC determined that ZAG voluntarily self-disclosed the apparent violations to OFAC, and that the apparent violations constitute a non-egregious case. The statutory maximum civil monetary penalty amount for the apparent violations was \$28,991,922, and the base civil monetary penalty amount was \$625,000.

During the time period in which the apparent violations occurred, ZAG's business focused on global sourcing and marketing of cement raw materials and providing strategic advisory services related to raw material selection for companies in the construction industry. On April 11, 2014, ZAG signed a supply contract with a company based in Tanzania (the “Purchaser”) and agreed to supply about 400,000 metric tons of cement clinker manufactured by a company based in India (the “Supplier”). Under the terms of the contract, ZAG was required to supply the Purchaser with a minimum of three shipments of cement clinker in 2014 and a minimum of five shipments in 2015 (about 50,000 metric tons per each shipment).

On or about June 26, 2014, the Supplier sent an email to ZAG's Managing Director of the Asia Pacific, Middle East, and East Africa Regions (“ZAG Managing Director”) that, due to a technical problem at its production plant, it would not have sufficient cement clinker to load onto ZAG's vessel on or about July 5, 2014. ZAG attempted to reschedule the date of its first shipment to the Purchaser but was unable to do so after the Purchaser objected to any delays and threatened to cancel the entire contract. The ZAG Managing Director subsequently identified a

These select settlement agreements were published by OFAC between 2019 and 2009.

2018 Information

- Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Zoltek Companies, Inc. 
- Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Yantai Jereh Oilfield Services Group Co. Ltd. 
- Settlement Agreement Made by and Between the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and Societe Generale S.A. 
- Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Ericsson, Inc. and Ericsson, AB 

2017 Information

- Dominica Maritime Registry, Inc. has received a Finding of Violation for violations of the Iranian Transactions Sanctions Regulations 
- Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and CSE Global Limited and CSE TransTel Pte. Ltd. 
- Zhongxing Telecommunications Equipment Corporation Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations 
- B Whale Corporation has received a Finding of Violation for violations of the Iranian Transactions Sanctions Regulations 

2016 Information

- AXA Equitable Life Insurance Company has received a Finding of Violation for violations of the Foreign Narcotics Kingpin Sanctions Regulations 
- Humana, Inc. has received a Finding of Violation for violations of the Foreign Narcotics Kingpin Sanctions Regulations 
- Compass Bank Receives a Finding of Violation Regarding Violations of the Foreign Narcotics Kingpin Sanctions Regulations 
- MasterCard International Incorporated Receives a Finding of Violation Regarding Violations of the Reporting, Procedures and Penalties Regulations 

311 ANNOUNCEMENTS

- [FinCEN Withdraws Section 311 Actions Against Latvia's VEF Banka](#)
- [Treasury Identifies Lebanese Canadian Bank Sal as a “Primary Money Laundering Concern”](#)
- [Treasury Wields PATRIOT Act Powers to Isolate Two Latvian Banks](#)
- [Fact Sheet Regarding the Treasury Department’s Use of Sanctions Authorized Under Section 311 of the USA PATRIOT ACT](#)
- [Treasury Department Rescinds Ukraine’s Designation as a Primary Money Laundering Concern](#)
- [Treasury Employs USA PATRIOT Act Authorities to Designate Two Foreign Banks as "Primary Money Laundering Concerns"](#)
- [Treasury Department Announces Proposed Anti-Money Laundering Countermeasure Against Nauru](#)
- [Treasury Designates Commercial Bank of Syria as Financial Institution of Primary Money Laundering Concern](#)
- [Treasury Department Designates Burma and Two Burmese Banks to be of “Primary Money Laundering Concern” and Announces Proposed Countermeasures](#)
- [Revocation of Designation of Ukraine as Primary Money Laundering Concern](#) 

Treasury Wields PATRIOT Act Powers to Isolate Two Latvian Banks Financial Institutions Identified as ♦Primary Money Laundering Concerns

4/21/2005

JS-2401

The U.S. Department of the Treasury today utilized *USA PATRIOT Act* powers to designate two Latvian financial institutions as "primary money laundering concerns." Multibanka and VEF Bank were named pursuant to Section 311 of the *Act* for money laundering activities and financial abuse by account holders and owners.

"The Treasury has judiciously and strategically utilized the power of Section 311 to isolate rogue actors that present money laundering concerns and risks to the U.S. financial sector," said Treasury Secretary John W. Snow. "Our use of this authority also alerts our global counterparts of specific concerns about real threats to the integrity of the international financial system."

In conjunction with this designation, Treasury's Financial Crimes Enforcement Network (FinCEN) issued proposed rules that when made final will prohibit U.S. financial institutions from establishing, maintaining, administering or managing any correspondent account in the United States for or on behalf of these two banks.

"These two Latvian banks represent a danger to the international community because they facilitate the placement and movement of dirty money in the global financial system," said Daniel Glaser, the Treasury's Deputy Assistant Secretary for Terrorist Financing and Financial Crimes. "We will continue to work closely with the Latvian government to crack down on crimes in their financial sector."

Multibanka

Headquartered in Riga, Multibanka is the oldest commercial bank in Latvia and is among the smaller of Latvia's 23 banks. Multibanka has four foreign offices (Russia, Ukraine and Belarus), five domestic branches and one leasing subsidiary called Multilizings. The Notice of Proposed Rulemaking issued today identifies several reasons for the designation of Multibanka as a primary money laundering concern:

- Multibanka offers confidential banking services and numbered accounts for non-Latvian customers. Reports substantiate that a significant portion of its business involves wiring money out of the country on behalf of its accountholders.
- Information available to the U.S. Government shows Multibanka has been used by Russian and other shell companies to facilitate financial crime by allowing criminals to disguise illegal proceeds in countries known for lax enforcement of anti-money laundering laws.
- According to information available to the U.S. Government, certain criminals use accounts at Multibanka to facilitate financial fraud schemes. Specifically, an individual involved in financial fraud reported carrying out large sum transactions through his account at Multibanka. In addition, an individual arrested in 2004 for his involvement in an access device fraud ring used an account at Multibanka to launder proceeds of his criminal activities.

VEF Bank

Headquartered in Riga, VEF is one of the smallest of Latvia's 23 banks. It has one subsidiary, Veiksmes I♦zings, which offers

Money Laundering



Money laundering generally refers to financial transactions in which criminals, including terrorist organizations, attempt to disguise the proceeds, sources or nature of their illicit activities. Money laundering facilitates a broad range of serious underlying criminal offenses and ultimately threatens the integrity of the financial system.

The United States Department of the Treasury is fully dedicated to combating all aspects of money laundering at home and abroad, through the mission of the Office of Terrorism and Financial Intelligence (TFI). TFI utilizes the Department's many assets - including a diverse range of legal authorities, core financial expertise, operational resources, and expansive relationships with the private sector, interagency and international communities - to identify and attack money laundering vulnerabilities and networks across the domestic and international financial systems."



NATIONAL TERRORIST FINANCING RISK ASSESSMENT

2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

INTRODUCTION 4

 PARTICIPANTS 5

 SOURCES 6

 METHODOLOGY 8

SECTION I: GLOBAL TERRORIST FINANCING THREAT 10

 A. OVERVIEW OF TERRORISM THREAT FACING THE UNITED STATES 11

 B. GLOBAL SOURCES OF TERRORIST FINANCING 14

SECTION II: COUNTERING TERRORIST FINANCING 19

 A. LAW ENFORCEMENT EFFORTS 20

 B. FINANCIAL/REGULATORY EFFORTS 22

 C. INTERNATIONAL ENGAGEMENT 23

 D. EXAMPLE OF SUCCESSFUL INTERAGENCY COORDINATION: RESPONSE TO THE ATTEMPTED TIMES SQUARE BOMBING 24

SECTION III: TERRORIST FINANCING VULNERABILITIES AND RISKS IN THE UNITED STATES 25

 A. RAISING FUNDS: VULNERABILITIES AND RISKS 26

 B. MOVING AND PLACING FUNDS: VULNERABILITIES AND RISKS 46

 C. POTENTIAL EMERGING THREATS 56

CONCLUSION 59

An analysis was conducted by the Department of the Treasury on terrorism and terrorism-related convictions between 2001 and 2014. Cases were flagged in which the defendant was charged with one or more of the below offenses:

- Title 18 of the U.S. Code, Section 2339A, which prohibits the provision of material support or resources knowing or intending that they are to be used in committing certain predicate violations associated with terrorism. Material support has been broadly defined to be any property, tangible or intangible, or service, and is not limited to physical transfers of assets (e.g. via a loan or something of value).
- Title 18 of the U.S. Code, Section 2339B, which prohibits knowingly providing material support or resources to an entity designated by the Secretary of State as a “foreign terrorist organization” (FTO), which currently includes 59 groups.⁶
- Title 18 of the U.S. Code, Section 2339C, which prohibits the unlawful and willful provision or collection of funds with the intention or knowledge they are to be used to carry out a terrorist attack.
- Title 18 of the U.S. Code, Section 2339D, which prohibits persons from receiving military-type training from, or on behalf of, an FTO. Under an aiding or abetting theory, anyone who finances another in receiving such training would be liable as a principal.
- Title 21 of the U.S. Code, Section 960a, which prohibits persons who have engaged in certain drug offenses from knowingly providing anything of pecuniary value to terrorists.
- Title 50 of the U.S. Code, Section 1705, which prohibits engaging in financial interactions with a person or entity that has been named as a Specially Designated Global Terrorist (SDGT), unless OFAC has issued a license permitting the transaction. This also prohibits making or receiving any contribution of funds, goods, or services to or for the benefit of an SDGT.
- Title 18 of the U.S. Code, Section 1960, which prohibits operating a money transmitting business without obtaining a state license, if one is required, or without registering with FinCEN.

TERRORIST FINANCE TRACKING PROGRAM (TFTP)

- Initiated after 9/11, enables Treasury Dept. to identify, track, and pursue terrorists and their networks. Involves tracking terrorist money flows and assists in efforts to uncover terrorist cells and map terrorist networks in the U.S. and internationally.
- U.S. Treasury Department issues subpoenas to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) – a Belgium-based company with U.S. offices that operates a worldwide messaging system used to transmit financial transaction information – seeking information on suspected international terrorists or their networks. Under the terms of the subpoenas, the U.S. Government may only review information as part of specific terrorism investigations.
- Based on information that identifies an individual or entity, the U.S. Government is able to conduct targeted searches against the limited subset of records provided by SWIFT in order to trace financial transactions related to suspected terrorist activity
- SWIFT information greatly enhances our ability to map out terrorist networks, often filling in missing links in an investigative chain. The U.S. Government acts on this information – and, for counter-terrorism purposes only, shares leads generated by the TFTP with relevant governments' counter-terrorism authorities – to target and disrupt the activities of terrorists and their supporters.
- By following the money, the TFTP has allowed the U.S. and our allies to identify and locate operatives and their financiers, chart terrorist networks, and help keep money out of their hands.
- The TFTP is firmly rooted in sound legal authority, based on statutory mandates and Executive Orders – including the International Emergency Economic Powers Act (IEEPA) and the United Nations Participation Act (UNPA).
- Does not involve data mining. Overseen by committee from major central banks e.g. Federal Reserve, Bank of England.

COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS)

*Interagency committee authorized to review certain transactions involving foreign investments in the U.S. to determine their impact on U.S. national security.

*Authorized by Section 721 of 1950 Defense Production Act (P.L. 81-774), implemented by Executive Order 11858 (May 7, 1975), and 31 CFR 800-801.

*Updated in 2018 by Foreign Investment Risk Review Modernization Act (FIRRMA) on Aug, 13, 2018 (Public Law 115-232 John McCain National Defense Authorization Act Sections 1701 et. seq.)

*CFIUS Members: Treasury Dept. (Chair), Depts. of Justice, Homeland Security, Commerce, Defense, State, Energy, U.S. Trade Rep., & Office of Science & Technology Policy,

*Additional participants, as required: Office of Management & Budget, Council of Economic Advisors, National Security Council, National Economic Council, & Homeland Security Council.

Process Overview - Voluntary Notice

Prior to filing a voluntary notice, parties may consult with CFIUS or submit a draft notice, as described in [Filing Instructions](#) section of this Web site, to ensure that the review will proceed as efficiently as possible. The CFIUS process generally begins formally when parties to a proposed or pending transaction jointly file a voluntary notice in accordance with the procedures stated in the regulations at § 800.401. The notice must include the information required in the regulations at § 800.402. Upon receiving the notice, the Staff Chairperson will promptly determine whether the notice satisfies the requirements for completeness as promulgated in the regulations. If the notice is complete, the Staff Chairperson will circulate the notice to all CFIUS members. A review period of up to 45 days begins on the next business day.

During the review period, CFIUS members examine the transaction in order to identify and address, as appropriate, any national security concerns that arise as a result of the transaction. During the review period, CFIUS members, through the Department of the Treasury as Committee Chair, may request additional information from the parties. Parties must respond to such follow-up requests within three business days of the request or within a longer time frame if the parties so request in writing and the Staff Chairperson grants that request in writing.



CFIUS Reform: Guidance on National Security Considerations

The U.S. Treasury Department, as chair of the Committee on Foreign Investment in the United States (CFIUS), and as required by the Foreign Investment & National Security Act of 2007, has issued guidance on the types of transactions that CFIUS has reviewed and that have presented national security considerations. The guidance also provides insight into how CFIUS identifies the national security effects of covered transactions.

Explains the relevance of national security considerations in the context of CFIUS reviews:

- *CFIUS's purpose:* Identify and address national security risk posed by covered transactions
- *National security risk:* Risk is a function of the interaction between threat and vulnerability, in light of the potential consequences of that interaction for U.S. national security
- *National security considerations:* Considerations are facts and circumstances, with respect to a covered transaction, that have potential national security implications.
- *Relevance of national security considerations:* CFIUS analyzes all national security considerations to assess whether a covered transaction poses national security risk. Transactions that present such considerations do not necessarily pose national security risk

Illustrates the types of transactions that have presented national security considerations:

- *Illustrative, not comprehensive:* Emphasizes that CFIUS considers all relevant facts and circumstances in each case, regardless of industry. Within the following two major categories, the guidance provides illustrations, not a comprehensive description:

- *Nature of the U.S. business*: For example, national security considerations have been presented because the U.S. business has government contracts, has operations relevant to U.S. national security, or deals in certain advanced technologies or goods and services controlled for export
- *Identity of the foreign person*: For example, national security considerations have been presented because of the track record of the foreign person acquiring control of the U.S. business, or the non-proliferation record of the person's country of origin
- *Foreign government control*: Constitutes a national security consideration, but the guidance addresses circumstances that may lessen its significance in a transaction
- *Corporate reorganizations*: Raise national security considerations only in exceptional cases

Clarifies the purpose of the guidance:

- CFIUS administers a voluntary notice system. Covered transactions reviewed by CFIUS receive a safe harbor from subsequent review. CFIUS may unilaterally review any covered transaction that does not have safe harbor, but it focuses solely on national security concerns
- The guidance does not set rules, nor discourage or encourage certain types of investment

For a link to the guidance, as well as additional information on CFIUS, please consult <http://www.treas.gov/offices/international-affairs/cfius/>.

12/01/2008

**COMMITTEE ON
FOREIGN INVESTMENT
IN THE UNITED STATES**

**ANNUAL REPORT
TO CONGRESS**

Section I: Covered Transactions

Introduction.....	1
A. Information Regarding 2015 Covered Transactions	2
B. Specific, Cumulative, and Trend Data for Covered Transactions, Withdrawals, and Investigations.....	3
C. Covered Transactions by Business Sector and Country.....	4
1. Covered Transactions by Business Sector of U.S. Companies, 2009-2015	4
2. Covered Transactions by Country or Economy, 2013-2015	16
D. Withdrawn Notices	20
E. Mitigation Measures	21
F. Perceived Adverse Effects of Covered Transactions	23

Section II: Critical Technologies

Introduction.....	27
Definitions and Methodologies	27
A. Whether There Is Credible Evidence of a Coordinated Strategy to Acquire Critical Technology Companies.....	28
1. Key Judgments	28
2. Summary of Foreign Merger and Acquisition (M&A) of U.S. Critical Technology Companies.....	28
3. Frequency of Activity by Countries and Companies	28
B. Whether Foreign Governments Used Espionage Activities to Obtain Commercial Secrets Related to Critical Technologies.....	31
1. Key Finding.....	31

Section III: Foreign Direct Investment in the United States by Countries that Boycott Israel or Do Not Ban Terrorist Organizations

Introduction.....	32
A. Summary of Findings and Conclusions.....	32
B. Study Methodology.....	33
1. Identification of Relevant Countries.....	33

Covered Transactions by Acquirer Home Country or Economy, 2013-2015

Country/Economy	2013	2014	2015	Total
Australia	0	4	4	8
Belgium	0	0	1	1
Brazil	1	0	0	1
British Virgin Islands	0	1	0	1
Canada	12	15	22	49
Cayman Islands	1	3	8	12
Chile	1	0	0	1
China	21	24	29	74
Denmark	0	0	1	1
Finland	0	1	2	3
France	7	6	8	21
Germany	4	9	1	14
Hong Kong	1	6	2	9
India	1	2	0	3
Indonesia	0	1	2	3
Ireland	1	1	2	4
Israel	1	5	3	9
Italy	0	0	2	2
Japan	18	10	12	40

Table II-1: Home Country of Foreign Acquirers of U.S. Critical Technology⁴

Country	Solo Deals	Joint Deals	Total Deals
Australia	3	0	3
Austria	1	0	1
Belgium	1	0	1
Brazil	1	0	1
BVI	1	1	2
Canada	20	0	20
Cayman Islands	1	2	3
Channel Islands	0	1	1
China	5	0	5
Denmark	1	0	1
Finland	2	0	2

Summary of the Foreign Investment Risk Review Modernization Act of 2018

The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) expands the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) to address growing national security concerns over foreign exploitation of certain investment structures which traditionally have fallen outside of CFIUS jurisdiction. Additionally, FIRRMA modernizes CFIUS's processes to better enable timely and effective reviews of covered transactions.

Key Provisions of FIRRMA:

- **Expands the scope of covered transactions**—FIRRMA broadens the purview of CFIUS by explicitly adding four new types of covered transactions: (1) a purchase, lease, or concession by or to a foreign person of real estate located in proximity to sensitive government facilities; (2) “other investments” in certain U.S. businesses that afford a foreign person access to material nonpublic technical information in the possession of the U.S. business, membership on the board of directors, or other decision-making rights, other than through voting of shares; (3) any change in a foreign investor’s rights resulting in foreign control of a U.S. business or an “other investment” in certain U.S. businesses; and (4) any other transaction, transfer, agreement, or arrangement designed to circumvent CFIUS jurisdiction.

MARCH 12, 2018 PRESIDENTIAL ORDER PROHIBITS BROADCOM FROM TAKING OVER QUALCOM FOR NATIONAL SECURITY REASONS BASED ON CFIUS RECOMMENDATION

REGARDING THE PROPOSED TAKEOVER OF QUALCOMM INCORPORATED BY BROADCOM LIMITED

By the authority vested in me as President by the Constitution and the laws of the United States of America, including section 721 of the Defense Production Act of 1950, as amended (section 721), 50 U.S.C. 4565, it is hereby ordered as follows:

Section 1. Findings. (a) There is credible evidence that leads me to believe that Broadcom Limited, a limited company organized under the laws of Singapore (Broadcom), along with its partners, subsidiaries, or affiliates, including Broadcom Corporation, a California corporation, and Broadcom Cayman L.P., a Cayman Islands limited partnership, and their partners, subsidiaries, or affiliates (together, the Purchaser), through exercising control of Qualcomm Incorporated (Qualcomm), a Delaware corporation, might take action that threatens to impair the national security of the United States; and

(b) Provisions of law, other than section 721 and the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), do not, in my judgment, provide adequate and appropriate authority for me to protect the national security in this matter.

Sec. 2. Actions Ordered and Authorized. On the basis of the findings set forth in section 1 of this order, considering the factors described in subsection 721(f) of

INTELLIGENCE BOARDS AND COMMISSIONS

- Numerous blue ribbon panels of experts have been established as boards or commissions to reveal overall U.S. intelligence agency operations or specific aspects of individual intelligence agencies activities.
- These can be appointed by presidential administrations or Congress.
- Many of their reports are in print FDLP collections or available online through Hathitrust catalog or other resources.
- These reports reflect expert opinion at the time on the strengths and weaknesses of U.S. intelligence agency programs.

Hoover Commission Report on Organization of the Executive Branch of
the Federal Government (1949) Chaired by former President Herbert
Hoover

	Preface	v
	First Letter of Transmittal	xi
	Reorganization Powers	xiii
I	General Management of the Executive Branch	i
II	Budgeting and Accounting	31
III	Statistical Activities	65
IV	Office of General Services	73
V	Federal Supply Activities	85
VI	Personnel Management	107
VII	Foreign Affairs	135
VIII	The National Security Organization	183
IX	Treasury Department	199
X	The Post Office	217
XI	Department of Agriculture	233
XII	Department of the Interior	261
XIII	Department of Commerce.	297
XIV	Department of Labor	319
XV	Medical Activities	333
XVI	Veterans' Affairs	357

Recommendation No. 18

The centralized intelligence unit in the State Department should be reorganized and reoriented, and intelligence advisers should be assigned to the regional action units.

The present misconception of the intelligence needs of the State Department must be eradicated. The creation of revitalized regional units on the action side should tend to correct the current deplorable attitude of the existing geographic offices toward intelligence. The reorientation of the centralized intelligence activities by de-emphasis of academic research and increased attention on current estimates and evaluations and to serving and making use of the Central Intelligence Agency is required. At present, except for the Special Projects Staff, the Biographic Information Division, and the routine library reference and collection functions, the existing intelligence unit appears to expend too much of its energies on projects which do not contribute sufficiently to the main work of the State Department.

The task force report contemplates the decentralization of the present area research personnel as intact units to the four new regional action units. This move would involve almost 5 percent of the personnel of the entire Department.

Interservice rivalries indicate a lack of understanding of the fact that military security depends upon cooperation and balance among the Army, Navy, and Air Force, and upon the creation of a genuinely unified military arm. There is a lack of close working relationships among such important elements as the Research and Development Board and the Joint Chiefs of Staff and the Central Intelligence Agency.

Some part of these weaknesses undoubtedly can be traced to the newness of the operation, but the Commission believes that they show serious organizational defects. The lack of central authority in the direction of the National Military Establishment, the rigid statutory structure established under the act, and divided responsibility have resulted in a failure to assert clear civilian control over the armed forces.

REPORT TO THE PRESIDENT BY THE COMMISSION ON CIA ACTIVITIES WITHIN THE UNITED STATES (1975)

Rockefeller Commission-Chaired by Vice-President Nelson Rockefeller. Future President Ronald Reagan was also a member.

Report to the President
by the
COMMISSION ON
CIA ACTIVITIES WITHIN
THE UNITED STATES

Part I.—Summary of the Investigation

Chapter	1. The Fundamental Issues.....	3
	2. The Need for Intelligence.....	6
	3. Summary of Findings, Conclusions, and Recommendations....	9

Part II. The CIA's Role and Authority

4. Intelligence and Related Activities by the United States before 1947.....	45
5. The Sources of CIA Authority.....	48
6. Legal Analysis.....	58

Part III. Supervision and Control of the CIA

7. External Controls.....	71
8. Internal Controls.....	83

Part IV. Significant Areas of Investigation

9. The CIA's Mail Intercepts.....	101
10. Intelligence Community Coordination.....	116
11. Special Operations Group—"Operation CHAOS".....	130
12. Protection of the Agency against Threats of Violence—Office	

A. Summary of Charges and Findings

The initial public charges were that the CIA's domestic activities had involved:

1. Large-scale spying on American citizens in the United States by the CIA, whose responsibility is foreign intelligence.
2. Keeping dossiers on large numbers of American citizens.
3. Aiming these activities at Americans who have expressed their disagreement with various government policies.

These initial charges were subsequently supplemented by others including allegations that the CIA:

- Had intercepted and opened personal mail in the United States for 20 years;
- Had infiltrated domestic dissident groups and otherwise intervened in domestic politics;
- Had engaged in illegal wiretaps and break-ins; and,
- Had improperly assisted other government agencies.

In addition, assertions have been made ostensibly linking the CIA to the assassination of President John F. Kennedy.

In accordance with its present guidelines, the CIA should not again engage in the testing of drugs on unsuspecting persons.

Recommendation (28)

Testing of equipment for monitoring conversations should not involve unsuspecting persons living within the United States.

Recommendation (29)

A civilian agency committee should be reestablished to oversee the civilian uses of aerial intelligence photography in order to avoid any concerns over the improper domestic use of a CIA-developed system.

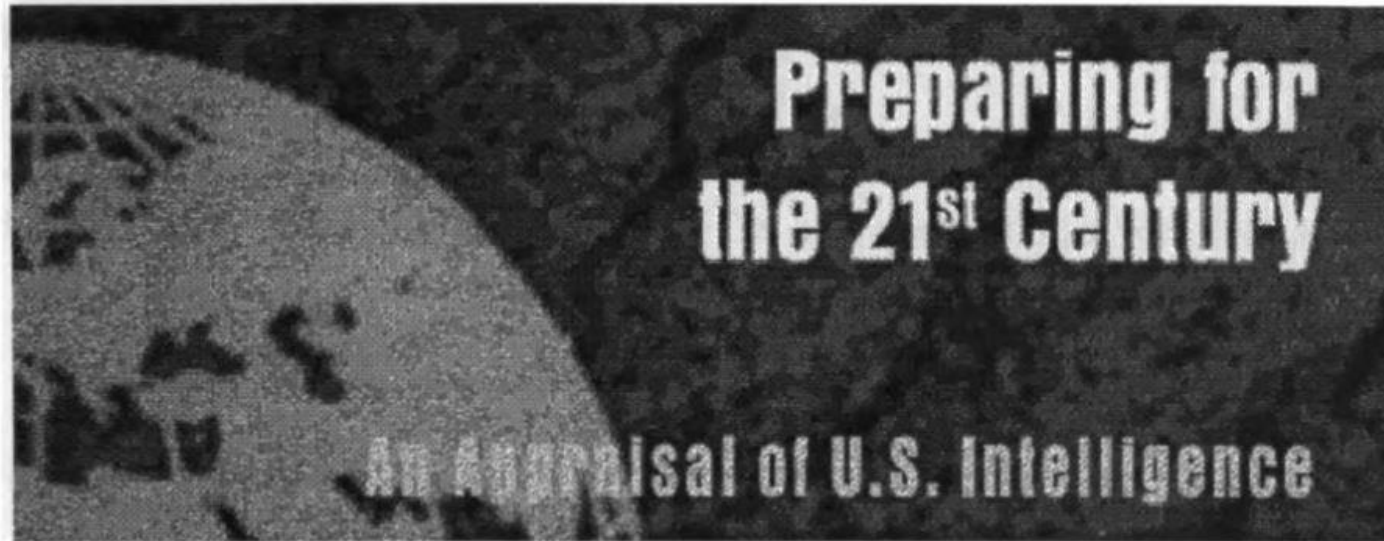
9. CIA Relationships With Other Federal, State, and Local Agencies (Chapter 17)

CIA operations touch the interest of many other agencies. The CIA, like other agencies of the government, frequently has occasion to give

Preparing for the 21st Century: An Appraisal of U.S. Intelligence (1996) Brown Rudman Commission-Chaired by Carter Admin. Sec. of Defense Harold Brown and former New Hampshire Senator Warren Rudman.

Preparing for the 21st Century

<http://www.access.gpo.gov/int/pdf/report.html>



March 1, 1996

Dedication

Preface

Executive Summary

Introduction

Chapter 1. The Need to Maintain an Intelligence Capability

Chapter 2. The Role of Intelligence

Chapter 3. The Need For Policy Guidance

Chapter 4. The Need for a Coordinated Response to Global Crime

Chapter 5. The Organizational Arrangements for the Intelligence Community

Chapter 6. The Central Intelligence Agency

Chapter 7. The Need for an Effective Budget Structure and Process

Chapter 8. Improving Intelligence Analysis

Chapter 9. The Need to "Right-Size" and Rebuild the Community

Chapter 10. Military Intelligence

Chapter 11. Space Reconnaissance and the Management of Technical Collection

Chapter 12. International Cooperation

Chapter 13. The Cost of Intelligence

Chapter 14. Accountability and Oversight

Epilogue

Additional Views of Senator John Warner

Acknowledgments

Overall Findings and Conclusions

The Commission concludes that the United States needs to maintain a strong intelligence capability. U.S. intelligence has made, and continues to make, vital contributions to the nation's security, informing its diplomacy and bolstering its defenses. While the focus provided by the superpower struggle of the Cold War has disappeared, there remain sound and important roles and missions for American intelligence.

At the same time, the performance of U.S. intelligence can be improved:

- ◆ Intelligence must be closer to those it serves. Intelligence agencies need better direction from the policy level, regarding both the roles they perform and what they collect and analyze. Policymakers need to appreciate to a greater extent what intelligence can offer them and be more involved in how intelligence capabilities are used. Intelligence must also be integrated more closely with other functions of government, such as law enforcement, to achieve shared objectives.**

1999 President's Foreign Intelligence Advisory Board (PFIAB) Report on DOE security problems

SCIENCE AT ITS BEST

SECURITY AT ITS WORST

**A Report on Security Problems at the
U.S. Department of Energy**

DOE COUNTERINTELLIGENCE AND SECURITY CHRONOLOGY

- 1976** U.S. Government assesses that China may step up efforts to acquire relevant nuclear technology.
- 1977** Department of Energy established, from the Energy Research and Development Administration, Federal Energy Administration, and elements of several Cabinet Departments.
- May:** Classified GAO report cites the need for an independent group to assess the adequacy of safeguards for nuclear material, and to assure the health and safety of the public from nuclear operations. In response to this and to DOE Inspector General reports, the Assistant Secretary for Defense Programs establishes an independent, inter-agency group to report to him on the adequacy of safeguards at weapons labs. The group finds that safeguards at sensitive facilities are not effective, while DOE's Office of Safeguards and Security was giving these facilities passing grades.
- August:** James R. Schlesinger becomes Secretary of Energy.
- 1979** Travel to PRC begins by U.S. persons associated with U.S. nuclear weapons program; travelers face Chinese elicitation efforts.
- January 1:** U.S. normalizes relationship with China.

INTELLIGENCE COMMUNITY DAMAGE ASSESSMENT OF CHINA'S ACQUISITION OF U.S. NUCLEAR WEAPONS INFORMATION

Chinese strategic nuclear efforts have focused on developing and deploying a survivable long-range missile force that can hold a significant portion of the U.S. and Russian populations at risk in a retaliatory strike. By at least the late 1970s the Chinese launched an ambitious collection program focused on the U.S., including its national laboratories, to acquire nuclear weapons technologies. By the 1980s China recognized that its second strike capability might be in jeopardy unless its force became more survivable. This probably prompted the Chinese to heighten their interest in smaller and lighter nuclear weapon systems to permit a mobile force.

China obtained by espionage classified U.S. nuclear weapons information that probably accelerated its program to develop future nuclear weapons. This collection program allowed China to focus successfully down critical paths and avoid less promising approaches to nuclear weapons designs.

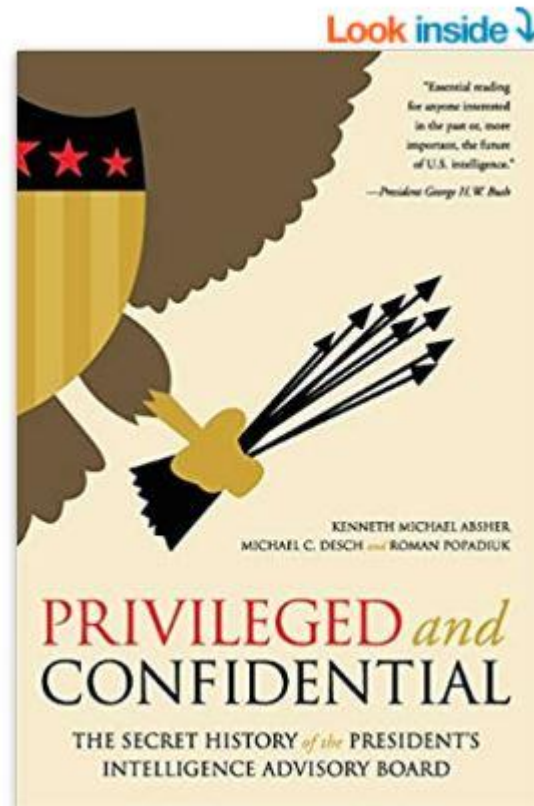
- China obtained at least basic design information on several modern U.S. nuclear reentry vehicles, including the Trident II (W-88).
- China also obtained information on a variety of U.S. weapon design concepts and weaponization features, including those of a neutron bomb.

Major DOE Field Facilities



SCHOLARLY WORK ON PRESIDENT'S INTELLIGENCE

ADVISORY BOARD (UNIVERSITY PRESS OF KENTUCKY, 2012)



PURDUE
UNIVERSITY

Libraries

U.S. national security and military/commercial concerns with the People's Republic of China (House Report 105-851) 3 vols. Cox report (1999) Rep. Chris Cox California. Dealt with Chinese espionage at DOE Labs.

VOLUME I

All-Volume Overview

CHAPTER 1

Commercial and Intelligence Operations: PRC Acquisition of U.S. Technology

CHAPTER 2

PRC Theft of U.S. Thermonuclear Weapons Design Information

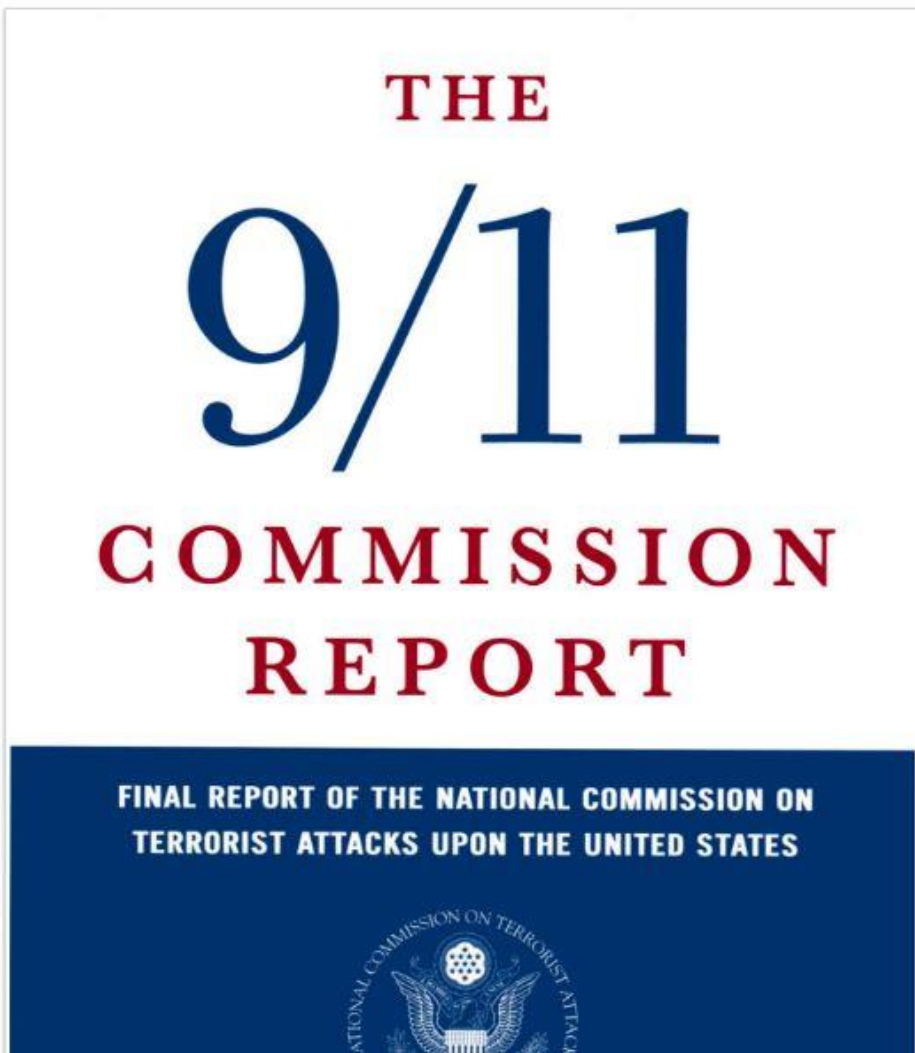
CHAPTER 3

High Performance Computers

CHAPTER 4

PRC Missile and Space Forces

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States



Description

The official Government edition of the Final Report of the National Commission on Terrorist Attacks Upon the United States (also known as the 9-11 Commission, an independent, bipartisan commission created by congressional legislation and the signature of President George W. Bush in late 2002), provides a full and complete account of the circumstances surrounding the September 11, 2001 terrorist attacks, including preparedness for and the immediate response to the attacks. Provides recommendations designed to guard against future attacks.

Physical Description

xviii, 567 p: ill., maps; 24 cm.

Creation Information

National Commission on Terrorist Attacks upon the United States July 22, 2004.

Context

1. “WE HAVE SOME PLANES” 1
 - 1.1 Inside the Four Flights 1
 - 1.2 Improvising a Homeland Defense 14
 - 1.3 National Crisis Management 35

2. THE FOUNDATION OF THE NEW TERRORISM 47
 - 2.1 A Declaration of War 47
 - 2.2 Bin Ladin’s Appeal in the Islamic World 48
 - 2.3 The Rise of Bin Ladin and al Qaeda (1988–1992) 55
 - 2.4 Building an Organization, Declaring
War on the United States (1992–1996) 59
 - 2.5 Al Qaeda’s Renewal in Afghanistan (1996–1998) 63

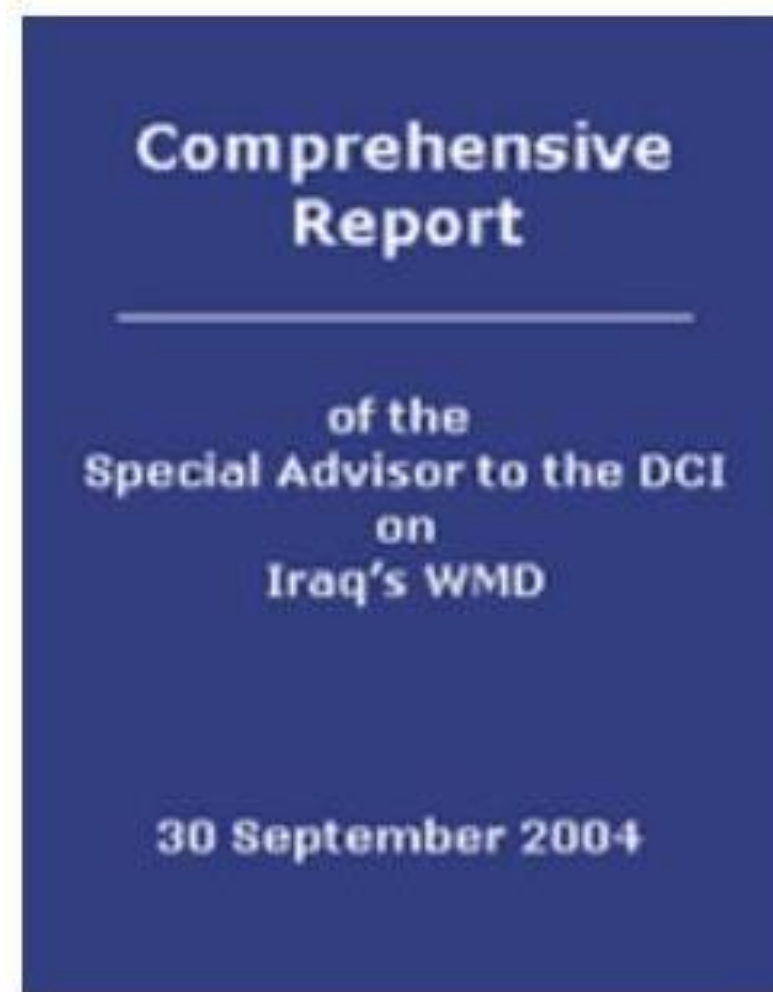
3. COUNTERTERRORISM EVOLVES 71
 - 3.1 From the Old Terrorism to the New:
The First World Trade Center Bombing 71
 - 3.2 Adaptation—and Nonadaptation—
in the Law Enforcement Community 73

We recommend significant changes in the organization of the government. We know that the quality of the people is more important than the quality of the wiring diagrams. Some of the saddest aspects of the 9/11 story are the outstanding efforts of so many individual officials straining, often without success, against the boundaries of the possible. Good people can overcome bad structures. They should not have to.

The United States has the resources and the people. The government should combine them more effectively, achieving unity of effort. We offer five major **recommendations** to do that:

- unifying strategic intelligence and operational planning against Islamist terrorists across the foreign-domestic divide with a National Counterterrorism Center;
- unifying the intelligence community with a new National Intelligence Director;

Duelfer Report (2004-2005) Report to Director of Central Intelligence on Iraq's Weapons of Mass Destruction-3 vols.



Acknowledgements

(12 September 2004 2330)

This report is the product of the hundreds of individuals who participated in the efforts of Iraq Survey Group (ISG): The Australian, British, and American soldiers, analysts, and support personnel who filled its ranks. They carried out their roles with distinction, and their work reflects creditably on the commitment of Washington, London, and Canberra to firmly support the mission throughout a long and difficult period.

Two of our colleagues gave their lives during ISG's field inspections. On April 26, Sgt. Sherwood J. Baker and Sgt. Lawrence A. Roukey died while providing security for one of the most critical ISG investigations when an explosion destroyed the facility being inspected. Their memory has been present throughout the creation of this report.

The analysts and case officers who came to Iraq, most for the first time, worked hard to develop the information to support this report. They labored long hours to develop intelligence reports and the text that became this report, a difficult task to which they responded with enthusiasm.

This report also builds upon the work of a broader universe of people who have striven to understand the role of Weapons of Mass Destruction in Iraq during the past decade or more. United Nations inspectors and analysts around the world have wrestled with this issue trying to sort out the truth and develop policies to mitigate suffering and avoid conflict. Hopefully this report will provide some answers or at least more data for constructive review.

Mention must be made of the Iraqis themselves. It is important for an outsider to understand

Contents

Key Findings.....	1
Who Made Iraq’s Strategic Decisions and Determined WMD Policy.....	5
Saddam’s Place in the Regime	5
The Apex of Power.....	5
Personalized Rule	5
Saddam’s Unsettled Lieutenants.....	5
A Few Key Players in an Insular Environment	7
Saddam Calls the Shots	8
Saddam Shows the Way.....	9
Harvesting Ideas and Advice in a Byzantine Setting.....	10
Weaving a Culture of Lies	11
Saddam Became Increasingly Inaccessible.....	11
Saddam’s Command By Violence	12
Saddam’s Effect on the Workings of the Iraqi Government	13
Suspicion of Structures.....	13
Powerless Structures.....	13
The Higher Committee	14
The Foreign Policy Committees	15
Saddam’s Grip on National Security and WMD Development.....	16
Saddam Holding Court.....	18
Saddam and Fiscal Policy.....	18

- ***The introduction of the Oil-For-Food program (OFF) in late 1996 was a key turning point for the Regime.*** OFF rescued Baghdad's economy from a terminal decline created by sanctions. The Regime quickly came to see that OFF could be corrupted to acquire foreign exchange both to further undermine sanctions and to provide the means to enhance dual-use infrastructure and potential WMD-related development.
- ***By 2000-2001, Saddam had managed to mitigate many of the effects of sanctions and undermine their international support.*** Iraq was within striking distance of a *de facto* end to the sanctions regime, both in terms of oil exports and the trade embargo, by the end of 1999.

Saddam wanted to recreate Iraq's WMD capability—which was essentially destroyed in 1991—after sanctions were removed and Iraq's economy stabilized, but probably with a different mix of capabilities to that which previously existed. Saddam aspired to develop a nuclear capability—in an incremental fashion, irrespective of international pressure and the resulting economic risks—but he intended to focus on ballistic missile and tactical chemical warfare (CW) capabilities.

- ***Iran was the pre-eminent motivator of this policy.*** All senior level Iraqi officials considered Iran to be Iraq's principal enemy in the region. The wish to balance Israel and acquire status and influence in the Arab world were also considerations, but secondary.
- ***Iraq Survey Group (ISG) judges that events in the 1980s and early 1990s shaped Saddam's belief in the value of WMD.*** In Saddam's view, WMD helped to save the Regime multiple times. He believed that during the Iran-Iraq war chemical weapons had halted Iranian ground offensives and that ballistic missile attacks on Tehran had broken its political will. Similarly, during Desert Storm, Saddam believed WMD had deterred Coalition Forces from pressing their attack beyond the goal of freeing Kuwait. WMD had even played a role in crushing the Shi'a revolt in the south following the 1991 cease-fire.
- ***The former Regime had no formal written strategy or plan for the revival of WMD after sanctions.*** Neither was there an identifiable group of WMD policy makers or planners separate from Saddam. Instead, his lieutenants understood WMD revival was his goal from their long association with Saddam and his infrequent, but firm, verbal comments and directions to them.

Report of the National Commission for the Review of the Research and Development Programs of the U.S. Intelligence Community (2013)

REPORT OF THE NATIONAL COMMISSION
FOR THE REVIEW OF THE RESEARCH AND
DEVELOPMENT PROGRAMS OF THE
UNITED STATES INTELLIGENCE COMMUNITY

Failure to properly appraise the extent of scientific developments in enemy countries may have more immediate and catastrophic consequences than failure in any other field of intelligence.

—Task Force Report on National Security Organization (the Eberstadt Report) (1948)

Failure to properly resource and use our own R&D to appraise, exploit, and counter the scientific and technical developments of our adversaries—including both state and non-state actors—may have more immediate and catastrophic consequences than failure in any other field of intelligence.

—National Commission for the Review of the Research and Development Programs of the United States Intelligence Community (2013)

Contents

Preface.....	1
SUMMARY OF FINDINGS AND RECOMMENDATIONS.....	3
The Threat from Global Scientific and Technical Knowledge.....	3
Strategic Objectives and Challenges.....	4
Broaden Scientific and Technical Intelligence.....	6
Enhance Integrated Intelligence.....	9
Empower R&D Leadership.....	10
Leverage People/Talent.....	12
Importance of R&D—Building the Future.....	15
APPENDICES	
Abbreviations.....	19
Legislation Pertinent to the Commission.....	20
List of Briefings.....	27
Commissioner Biographies.....	33
Acknowledgments.....	37

advantages. The United States faces increasing risk from threats against which the IC could have severely limited warning, deterrence, or agility to develop effective countermeasures.

The Threat from Global Scientific and Technical Knowledge

Our adversaries' use of S&T increasingly challenges IC capabilities in critical areas, including:

- *Cryptography.* The availability and strength of high-grade encryption schemes continue to expand.
- *Assured Space Access.* Foreign countries continue to develop new technologies and methods for disrupting our space assets, necessitating the development of resilient approaches.
- *Cyber Attack and Defense.* As cyber attacks grow in scale and scope, we struggle to defend against this rising threat.
- *Nuclear Technology and Forensics.* The proliferation of nuclear materials and technology will remain a high-priority national security threat.
- *Global Supply Chains.* Production and distribution chains are increasingly vulnerable to a variety of actions, including intentional disruptions.
- *All-Source Data Analytics.* The volume of data is challenging our ability to process and use it.

Exacerbating these challenges are U.S. policies that weaken the U.S. R&D talent base. As scientific and technical knowledge and the resulting economic growth spread around the world,

Broaden Scientific and Technical Intelligence

Finding 1: The Commission found a limited effort by the IC to discern and exploit the strategic R&D—especially non-military R&D—intentions and capabilities of our adversaries, and to counter our adversaries’ theft or purchase of U.S. technology.

Recommendation 1: Conduct comprehensive strategic scientific and technical intelligence (S&TI); use it for IC R&D planning and resource allocation.

Enhance Integrated Intelligence

Finding 2: The Commission found that while the traditional ways and means of collecting and analyzing intelligence remain useful and necessary, emerging and future threats cannot be addressed without Enhanced Integrated Intelligence capabilities that enable shared, discoverable data for analysis and shared, discoverable information for decisionmakers.

Recommendation 2: Focus advanced IC R&D on Enhanced Integrated Intelligence approaches—methods that integrate diverse sources and expertise and that employ automated capabilities to tag, discover, access, and aggregate both data and analyzed information.

Empower R&D Leadership

Finding 3: The Commission found that there is inadequate IC R&D strategic planning and inadequate awareness of IC R&D investment plans and programs.

Recommendation 3: Empower IC R&D leadership to develop a comprehensive R&D strategy and oversee R&D resource allocation.

BENEFITS OF THESE INTELLIGENCE RESOURCES

- Gaining enhanced understanding of the information resources produced by multiple agencies covering U.S. intelligence.
- Understanding how energy, homeland security, cyber security, foreign policy, economic intelligence, and governmental commission information resources enhance understanding of historic and contemporary U.S. intelligence analysis, activities, and operations.
- Increasing awareness of the multiple subject areas involved in conducting and assessing intelligence operations.
- Understanding the historical evolution, contemporary trends, and emerging trends affecting U.S. intelligence operations.
- Gaining enhanced appreciation of the skills, challenges, opportunities, and ambiguities facing those engaged in intelligence activities.
- Being appreciative that significant amounts of information on U.S. intelligence activities are publicly available.