

FOIA Marker

This is not a textual record. This FOIA Marker indicates that material has been removed during FOIA processing by George W. Bush Presidential Library staff.

National Security Council - Legal Adviser

Sadoff, David

Stack:	Row:	Sect.:	Shelf:	Pos.:	FRC ID:	Location or Hollinger ID:
V	13	6	2	2	35336	1000003974

Folder Title:

Information Sharing: Intelligence Reform Legislation

Withdrawn/Redacted Material

The George W. Bush Library

DOCUMENT NO.	FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
003	Email	Re: Info-Sharing Provisions of Collins-Lieberman Bill - To: David Sadoff	1	10/04/2004	P3/b3; P5; b7f;
004	Email	Re: More... - To: David Sadoff	2	10/04/2004	P3/b3; P5; b7f;
005	Letter	[Letter] - To: Susan M. Collins, et al - From: Thomas Ridge, et al	4	04/13/2004	P3/b3; P6/b6; b7c; b7f;
006	Draft	Memorandum	7	N.D.	P5;

COLLECTION TITLE:

National Security Council - Legal Adviser

SERIES:

Sadoff, David

FOLDER TITLE:

Information Sharing: Intelligence Reform Legislation

FRC ID:

35336

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

- A. Closed by Executive Order 13526 governing access to national security information.
- B. Closed by statute or by the agency which originated the document.
- C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Records Not Subject to FOIA

Court Sealed - The document is withheld under a court seal and is not subject to the Freedom of Information Act.

"(c) CONSULTATION WITH DNI IN CERTAIN POSITIONS.—(1) In the event of a vacancy in a position referred to in paragraph (2), the head of the department or agency having jurisdiction over the position shall consult with the Director of National Intelligence before appointing an individual to fill the vacancy or recommending to the President an individual to be nominated to fill the vacancy.

"(2) Paragraph (1) applies to the following positions:

"(A) The Director of the Defense Intelligence Agency.

"(B) The Assistant Commandant of the Coast Guard for Intelligence."

SEC. 1015. EXECUTIVE SCHEDULE MATTERS.

(a) EXECUTIVE SCHEDULE LEVEL I.—Section 5312 of title 5, United States Code, is amended by adding the end the following new item:

"Director of National Intelligence."

(b) EXECUTIVE SCHEDULE LEVEL II.—Section 5313 of title 5, United States Code, is amended by adding at the end the following new items:

"Principal Deputy Director of National Intelligence.

"Director of the National Counterterrorism Center.

"Director of the National Counter Proliferation Center."

(c) EXECUTIVE SCHEDULE LEVEL IV.—Section 5315 of title 5, United States Code, is amended—

(1) by striking the item relating to the Assistant Directors of Central Intelligence; and

(2) by adding at the end the following new item:

"General Counsel of the Office of the National Intelligence Director."

SEC. 1016. INFORMATION SHARING.

(a) DEFINITIONS.—In this section:

(1) INFORMATION SHARING COUNCIL.—The term "Information Sharing Council" means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection (g).

(2) INFORMATION SHARING ENVIRONMENT; ISE.—The terms "information sharing environment" and "ISE" mean an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section.

(3) PROGRAM MANAGER.—The term "program manager" means the ~~program manager~~ designated under subsection (f).

(4) TERRORISM INFORMATION.—The term "terrorism information" means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

(A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;

(substance
Same as in E.O.)

(B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

(C) communications of or by such groups or individuals; or

(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

(b) **INFORMATION SHARING ENVIRONMENT.**—

(1) **ESTABLISHMENT.**—~~The President~~ shall—

(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

(2) **ATTRIBUTES.**—The President shall, through the structures described in subparagraphs (B) and (C) of paragraph (1), ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that—

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties; and

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.

(c) **PRELIMINARY REPORT.**—Not later than 180 days after the date of the enactment of this Act, the program manager shall, in consultation with the Information Sharing Council—

Freeable on Info Shg

120 days - Respt PM

180 days - PM, JSC

Submit issues, and not revise

270 days - Pres review guidelines + reports

360 days - Pres reports to Congress on implementation plan

720 days - Pres submits to Congress on state of ISE + Info Shg across Fed govt

(1) submit to the President and Congress a description of the technological, legal, and policy issues presented by the creation of the ISE, and the way in which these issues will be addressed;

(2) establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information; and

(3) conduct a review of relevant current Federal agency capabilities, databases, and systems for sharing information.

(d) GUIDELINES AND REQUIREMENTS.—As soon as possible, but in no event later than 270 days after the date of the enactment of this Act, the President shall—

(1) leverage all ongoing efforts consistent with establishing the ISE and issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;

(2) in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, issue guidelines that—

(A) protect privacy and civil liberties in the development and use of the ISE; and

(B) shall be made public, unless nondisclosure is clearly necessary to protect national security; and

(3) require the heads of Federal departments and agencies to promote a culture of information sharing by—

(A) reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval, consistent with applicable laws and regulations; and

(B) providing affirmative incentives for information sharing.

(e) IMPLEMENTATION PLAN REPORT.—Not later than one year after the date of the enactment of this Act, the President shall, with the assistance of the program manager, submit to Congress a report containing an implementation plan for the ISE. The report shall include the following:

(1) A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.

(2) A description of the impact on enterprise architectures of participating agencies.

(3) A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.

(4) A project plan for designing, testing, integrating, deploying, and operating the ISE.

(5) The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized.

(6) Objective, systemwide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.

(7) A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.

(8) A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.

(9) The recommendations of the program manager, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information.

(10) A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with—

(A) the authority of the Director of National Intelligence under this title, and the amendments made by this title, to set standards for information sharing throughout the intelligence community; and

(B) the authority of the Secretary of Homeland Security and the Attorney General, and the role of the Department of Homeland Security and the Attorney General, in coordinating with State, local, and tribal officials and the private sector.

(11) The recommendations of the program manager, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of program manager should continue to remain in existence.

(f) **PROGRAM MANAGER.—**

(1) **DESIGNATION.**—Not later than 120 days after the date of the enactment of this Act, with notification to Congress, the President shall designate an individual as the program manager responsible for information sharing across the Federal Government. The individual designated as the program manager shall serve as program manager during the two-year period beginning on the date of designation under this paragraph unless sooner removed from service and replaced by the President (at the President's sole discretion). The program manager shall have and exercise governmentwide authority. ✓

(2) **DUTIES AND RESPONSIBILITIES.—**

(A) **IN GENERAL.**—The program manager shall, in consultation with the Information Sharing Council—

(i) plan for and oversee the implementation of, and manage, the ISE;

(ii) assist in the development of policies, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the ISE; and

(iii) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

(B) **CONTENT OF POLICIES, PROCEDURES, GUIDELINES, RULES, AND STANDARDS.**—The policies, procedures, guidelines, rules, and standards under subparagraph (A)(ii) shall—

(i) take into account the varying missions and security requirements of agencies participating in the ISE;

(ii) address development, implementation, and oversight of technical standards and requirements;

(iii) take into account ongoing and planned efforts that support development, implementation and management of the ISE;

(iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community and the law enforcement community;

(v) address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments;

(vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

(vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and

(viii) ensure the protection of privacy and civil liberties.

(g) **INFORMATION SHARING COUNCIL.**—

(1) **ESTABLISHMENT.**—There is established an Information Sharing Council that shall assist the President and the program manager in their duties under this section. The Information Sharing Council shall serve during the two-year period beginning on the date of the initial designation of the program manager by the President under subsection (f)(1), unless sooner removed from service and replaced by the President (at the sole discretion of the President) with a successor body.

(2) **SPECIFIC DUTIES.**—In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall—

(A) advise the President and the program manager in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE;

(B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the ISE;

(C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems,

and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the re-direction of existing resources to support the ISE;

(D) identify gaps, if any, between existing technologies, programs and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment;

(E) recommend solutions to address any gaps identified under subparagraph (D);

(F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments; and

(G) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.

(3) **CONSULTATION.**—In performing its duties, the Information Sharing Council shall consider input from persons and entities outside the Federal Government having significant experience and expertise in policy, technical matters, and operational matters relating to the ISE.

(4) **INAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.**—The Information Sharing Council shall not be subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App.).

(h) **PERFORMANCE MANAGEMENT REPORTS.**—

(1) **IN GENERAL.**—Not later than two years after the date of the enactment of this Act, and annually thereafter, the President shall submit to Congress a report on the state of the ISE and of information sharing across the Federal Government. ✓

(2) **CONTENT.**—Each report under this subsection shall include—

(A) a progress report on the extent to which the ISE has been implemented, including how the ISE has fared on the performance measures and whether the performance goals set in the preceding year have been met;

(B) objective system-wide performance goals for the following year;

(C) an accounting of how much was spent on the ISE in the preceding year;

(D) actions taken to ensure that procurement of and investments in systems and technology are consistent with the implementation plan for the ISE;

(E) the extent to which all terrorism watch lists are available for combined searching in real time through the ISE and whether there are consistent standards for placing individuals on, and removing individuals from, the watch lists, including the availability of processes for correcting errors;

(F) the extent to which State, tribal, and local officials are participating in the ISE;

(G) the extent to which private sector data, including information from owners and operators of critical infrastructure, is incorporated in the ISE, and the extent to

which individuals and entities outside the government are receiving information through the ISE;

(H) the measures taken by the Federal government to ensure the accuracy of information in the ISE, in particular the accuracy of information about individuals;

(I) an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections; and

(J) an assessment of the security protections used in the ISE.

(i) AGENCY RESPONSIBILITIES.—The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall—

(1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (f);

(2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;

(3) ensure full department or agency cooperation in the development of the ISE to implement governmentwide information sharing; and

(4) submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

(j) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section \$20,000,000 for each of fiscal years 2005 and 2006.

SEC. 1017. ALTERNATIVE ANALYSIS OF INTELLIGENCE BY THE INTELLIGENCE COMMUNITY.

(a) IN GENERAL.—Not later than 180 days after the effective date of this Act, the Director of National Intelligence shall establish a process and assign an individual or entity the responsibility for ensuring that, as appropriate, elements of the intelligence community conduct alternative analysis (commonly referred to as “red-team analysis”) of the information and conclusions in intelligence products.

(b) REPORT.—Not later than 270 days after the effective date of this Act, the Director of National Intelligence shall provide a report to the Select Committee on Intelligence of the Senate and the Permanent Select Committee of the House of Representatives on the implementation of subsection (a).

SEC. 1018. PRESIDENTIAL GUIDELINES ON IMPLEMENTATION AND PRESERVATION OF AUTHORITIES.

The President shall issue guidelines to ensure the effective implementation and execution within the executive branch of the authorities granted to the Director of National Intelligence by this title and the amendments made by this title, in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments of the United States Government concerning such departments, including, but not limited to:

"(6) The Director of National Intelligence shall establish requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for national intelligence purposes, except that the Director shall have no authority to direct or undertake electronic surveillance or physical search operations pursuant to that Act unless authorized by statute or Executive order.

"(7) The Director of National Intelligence shall perform such other functions as the President may direct.

"(8) Nothing in this title shall be construed as affecting the role of the Department of Justice or the Attorney General under the Foreign Intelligence Surveillance Act of 1978.

"(g) INTELLIGENCE INFORMATION SHARING.—(1) The Director of National Intelligence shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements. The Director of National Intelligence shall—

"(A) establish uniform security standards and procedures;

"(B) establish common information technology standards, protocols, and interfaces;

"(C) ensure development of information technology systems that include multi-level security and intelligence integration capabilities;

"(D) establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;

"(E) develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture; and

"(F) have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program.

"(2) The President shall ensure that the Director of National Intelligence has all necessary support and authorities to fully and effectively implement paragraph (1).

"(3) Except as otherwise directed by the President or with the specific written agreement of the head of the department or agency in question, a Federal agency or official shall not be considered to have met any obligation to provide any information, report, assessment, or other material (including unevaluated intelligence information) to that department or agency solely by virtue of having provided that information, report, assessment, or other material to the Director of National Intelligence or the National Counterterrorism Center.

"(4) Not later than February 1 of each year, the Director of National Intelligence shall submit to the President and to the Congress an annual report that identifies any statute, regulation, policy, or practice that the Director believes impedes the ability of the Director to fully and effectively implement paragraph (1).

- DNI
- intell inf
- EC only

1 (6) Strategic analysis.

2 (7) Intelligence program and budget manage-
3 ment.

4 (8) The intelligence workforce.

5 (9) Any other responsibilities specified by the
6 Director of the Federal Bureau of Investigation or
7 specified by law.

8 (d) STAFF.—The Directorate of Intelligence shall
9 consist of such staff as the Director of the Federal Bureau
10 of Investigation considers appropriate for the activities of
11 the Directorate.

12 **SEC. 207. INFORMATION SHARING.**

13 (a) DEFINITIONS.—In this section:

14 (1) EXECUTIVE COUNCIL.—The term “Execu-
15 tive Council” means the Executive Council on Infor-
16 mation Sharing established under subsection (h).

17 (2) HOMELAND SECURITY INFORMATION.—The
18 term “homeland security information” means all in-
19 formation, whether collected, produced, or distrib-
20 uted by intelligence, law enforcement, military,
21 homeland security, or other activities relating to—

22 (A) the existence, organization, capabili-
23 ties, plans, intentions, vulnerabilities, means of
24 finance or material support, or activities of for-
25 eign or international terrorist groups or individ-

1 nals, or of domestic groups or individuals in-
2 volved in transnational terrorism;

3 (B) threats posed by such groups or indi-
4 viduals to the United States, United States per-
5 sons, or United States interests, or to those of
6 other nations;

7 (C) communications of or by such groups
8 or individuals; or

9 (D) groups or individuals reasonably be-
10 lieved to be assisting or associated with such
11 groups or individuals.

12 (3) ENVIRONMENT.—The term “Environment”
13 means the Information Sharing Environment as de-
14 scribed under subsection (c).

15 (b) FINDINGS.—Consistent with the report of the Na-
16 tional Commission on Terrorist Attacks upon the United
17 States, Congress makes the following findings:

18 (1) The effective use of information, from all
19 available sources, is essential to the fight against
20 terror and the protection of our homeland. The big-
21 gest impediment to all-source analysis, and to a
22 greater likelihood of “connecting the dots”, is resist-
23 ance to sharing information.

24 (2) The United States Government has access
25 to a vast amount of information, including not only

1 traditional intelligence but also other government
2 databases, such as those containing customs or im-
3 migration information. However, the United States
4 Government has a weak system for processing and
5 using the information it has.

6 (3) In the period preceding September 11,
7 2001, there were instances of potentially helpful in-
8 formation that was available but that no person
9 knew to ask for; information that was distributed
10 only in compartmented channels, and information
11 that was requested but could not be shared.

12 (4) Current security requirements nurture over-
13 classification and excessive compartmentalization of
14 information among agencies. Each agency's incentive
15 structure opposes sharing, with risks, including
16 criminal, civil, and administrative sanctions, but few
17 rewards for sharing information.

18 (5) The current system, in which each intel-
19 ligence agency has its own security practices, re-
20 quires a demonstrated "need to know" before shar-
21 ing. This approach assumes that it is possible to
22 know, in advance, who will need to use the informa-
23 tion. An outgrowth of the cold war, such a system
24 implicitly assumes that the risk of inadvertent dis-
25 closure outweighs the benefits of wider sharing.

1 Such assumptions are no longer appropriate. Al-
2 though counterintelligence concerns are still real, the
3 costs of not sharing information are also substantial.
4 The current "need-to-know" culture of information
5 protection needs to be replaced with a "need-to-
6 share" culture of integration.

7 (6) A new approach to the sharing of intel-
8 ligence and homeland security information is ur-
9 gently needed. An important conceptual model for a
10 new "trusted information network" is the System-
11 wide Homeland Analysis and Resource Exchange
12 (SHARE) Network proposed by a task force of lead-
13 ing professionals assembled by the Markle Founda-
14 tion and described in reports issued in October 2002
15 and December 2003.

16 (7) No single agency can create a meaningful
17 information sharing system on its own. Alone, each
18 agency can only modernize stovepipes, not replace
19 them. Presidential leadership is required to bring
20 about governmentwide change.

21 (c) INFORMATION SHARING ENVIRONMENT.—

22 (1) ESTABLISHMENT.—The President shall es-
23 tablish a trusted information network and secure in-
24 formation sharing environment to promote sharing
25 of intelligence and homeland security information in

1 a manner consistent with national security and the
2 protection of privacy and civil liberties, and based on
3 clearly defined and consistently applied policies and
4 procedures, and valid investigative, analytical or
5 operational requirements.

6 (2) ATTRIBUTES.—The Environment shall pro-
7 mote coordination, communication and collaboration
8 of people and information among all relevant Fed-
9 eral departments and agencies, State, tribal, and
10 local authorities, and relevant private sector entities,
11 including owners and operators of critical infrastruc-
12 ture, by using policy guidelines and technologies that
13 support—

14 (A) a decentralized, distributed, and co-
15 ordinated environment that connects existing
16 systems where appropriate and allows users to
17 share information among agencies, between lev-
18 els of government, and, as appropriate, with the
19 private sector;

20 (B) the sharing of information in a form
21 and manner that facilitates its use in analysis,
22 investigations and operations;

23 (C) building upon existing systems capa-
24 bilities currently in use across the Government;

1 (D) utilizing industry best practices, in-
2 cluding minimizing the centralization of data
3 and seeking to use common tools and capabili-
4 ties whenever possible;

5 (E) employing an information access man-
6 agement approach that controls access to data
7 rather than to just networks;

8 (F) facilitating the sharing of information
9 at and across all levels of security by using pol-
10 icy guidelines and technologies that support
11 writing information that can be broadly shared;

12 (G) providing directory services for locat-
13 ing people and information;

14 (H) incorporating protections for individ-
15 uals' privacy and civil liberties;

16 (I) incorporating strong mechanisms for
17 information security and privacy and civil lib-
18 erties guideline enforcement in order to enhance
19 accountability and facilitate oversight,
20 including—

21 (i) multifactor authentication and ac-
22 cess control;

23 (ii) strong encryption and data protec-
24 tion;

25 (iii) immutable audit capabilities;

1 (iv) automated policy enforcement;

2 (v) perpetual, automated screening for
3 abuses of network and intrusions; and

4 (vi) uniform classification and han-
5 dling procedures;

6 (J) compliance with requirements of appli-
7 cable law and guidance with regard to the plan-
8 ning, design, acquisition, operation, and man-
9 agement of information systems;

10 (K) permitting continuous system up-
11 grades to benefit from advances in technology
12 while preserving the integrity of stored data;
13 and

14 (L) utilizing privacy-enhancing tech-
15 nologies that minimize the inappropriate dis-
16 semination and disclosure of personally identifi-
17 able information.

18 (d) IMMEDIATE ACTIONS.—Not later than 180 days
19 after the date of the enactment of this Act, the principal
20 officer as designated in subsection 206(g), in consultation
21 with the Executive Council, shall—

22 (1) submit to the President and to Congress a
23 description of the technological, legal, and policy
24 issues presented by the creation of the Environment

1 described in subsection (c), and the way in which
2 these issues will be addressed;

3 (2) establish electronic directory services to as-
4 sist in locating in the Federal Government intel-
5 ligence and homeland security information and peo-
6 ple with relevant knowledge about intelligence and
7 homeland security information; and

8 (3) conduct a review of relevant current Federal
9 agency capabilities, including—

10 (A) a baseline inventory of current Federal
11 systems that contain intelligence or homeland
12 security information;

13 (B) the money currently spent to maintain
14 those systems; and

15 (C) identification of other information that
16 should be included in the Environment.

17 (e) GUIDELINES AND REQUIREMENTS.—As soon as
18 possible, but in no event later than 270 days after the
19 date of the enactment of this Act, the President shall—

20 (1) in consultation with the Executive Council,
21 issue guidelines—

22 (A) for acquiring, accessing, sharing, and
23 using information, including guidelines to en-
24 sure that information is provided in its most
25 shareable form, such as by separating out data

1 from the sources and methods by which that
2 data are obtained; and

3 (B) issue guidelines on classification policy
4 and handling procedures across Federal agen-
5 cies, including commonly accepted processing
6 and access controls, in the course of which re-
7 view, the President may consider any comments
8 submitted by the Select Committee on Intel-
9 ligence, the Committee on Armed Services, the
10 Committee on Foreign Relations of the Senate,
11 and the Permanent Select Committee on Intel-
12 ligence, the Committee on Armed Services, and
13 the Committee on International Relations of the
14 House of Representatives regarding—

15 (i) the scope of the review the Presi-
16 dent should undertake in formulating the
17 guidelines under this subparagraph; and

18 (ii) the substance of what guidelines
19 should be issued.

20 (2) in consultation with the Privacy and Civil
21 Liberties Oversight Board established under section
22 211, issue guidelines that—

23 (A) protect privacy and civil liberties in the
24 development and use of the Environment; and

1 (B) shall be made public, unless, and only
2 to the extent that, nondisclosure is clearly nec-
3 essary to protect national security; and

4 (3) require the heads of Federal departments
5 and agencies to promote a culture of information
6 sharing by—

7 (A) reducing disincentives to information
8 sharing, including overclassification of informa-
9 tion and unnecessary requirements for origi-
10 nator approval; and

11 (B) providing affirmative incentives for in-
12 formation sharing, such as the incorporation of
13 information sharing performance measures into
14 agency and managerial evaluations, and em-
15 ployee awards for promoting innovative infor-
16 mation sharing practices.

17 (f) ENTERPRISE ARCHITECTURE AND IMPLEMENTA-
18 TION PLAN.—Not later than 1 year after the date of the
19 enactment of this Act, the President shall submit to Con-
20 gress an enterprise architecture and implementation plan
21 for the Environment. The enterprise architecture and im-
22 plementation plan shall be prepared by the principal offi-
23 cer in consultation with the Executive Council and shall
24 include—

1 (1) a description of the parameters of the pro-
2 posed Environment, including functions, capabilities,
3 and resources;

4 (2) a delineation of the roles of the Federal de-
5 partments and agencies that will participate in the
6 development of the Environment, including identi-
7 fication of any agency that will build the infrastruc-
8 ture needed to operate and manage the Environment
9 (as distinct from the individual agency components
10 that are to be part of the Environment), with the
11 delineation of roles to be consistent with—

12 (A) the authority of the National Intel-
13 ligence Director under this Act to set standards
14 for information sharing and information tech-
15 nology throughout the intelligence community;
16 and

17 (B) the authority of the Secretary of
18 Homeland Security and the role of the Depart-
19 ment of Homeland Security in coordinating
20 with State, tribal, and local officials and the
21 private sector;

22 (3) a description of the technological require-
23 ments to appropriately link and enhance existing
24 networks and a description of the system design that
25 will meet these requirements;

1 (4) an enterprise architecture that—

2 (A) is consistent with applicable laws and
3 guidance with regard to planning, design, acqui-
4 sition, operation, and management of informa-
5 tion systems;

6 (B) will be used to guide and define the
7 development and implementation of the Envi-
8 ronment; and

9 (C) addresses the existing and planned en-
10 terprise architectures of the departments and
11 agencies participating in the Environment;

12 (5) a description of how privacy and civil lib-
13 erties will be protected throughout the design and
14 implementation of the Environment;

15 (6) objective, systemwide performance measures
16 to enable the assessment of progress toward achiev-
17 ing full implementation of the Environment;

18 (7) a plan, including a time line, for the devel-
19 opment and phased implementation of the Environ-
20 ment;

21 (8) total budget requirements to develop and
22 implement the Environment, including the estimated
23 annual cost for each of the 5 years following the
24 date of the enactment of this Act;

1 (9) an estimate of training requirements needed
2 to ensure that the Environment will be adequately
3 implemented and property utilized;

4 (10) an analysis of the cost to State, tribal, and
5 local governments and private sector entities for
6 equipment and training needed to effectively utilize
7 the Environment; and

8 (11) proposals for any legislation that the Di-
9 rector of Management and Budget determines nec-
10 essary to implement the Environment.

11 (g) RESPONSIBILITIES OF EXECUTIVE COUNCIL FOR
12 INFORMATION SHARING ENVIRONMENT.—Not later than
13 120 days after the date of enactment, with notification
14 to Congress, the President shall designate an individual
15 as the principal officer responsible for information sharing
16 across the Federal government. That individual shall have
17 and exercise governmentwide authority and have manage-
18 ment expertise in enterprise architecture, information
19 sharing, and interoperability.

20 (1) ADDITIONAL DUTIES AND RESPONSIBIL-
21 ITIES.—

22 (A) IN GENERAL.—The principal officer
23 designated under this subsection, in consulta-
24 tion with the Executive Council, shall—

1 (i) implement and manage the Envi-
2 ronment;

3 (ii) develop and implement policies,
4 procedures, guidelines, rules, and stand-
5 ards as appropriate to foster the develop-
6 ment and proper operation of the Environ-
7 ment; and

8 (iii) assist, monitor, and assess the
9 implementation of the Environment by
10 Federal departments and agencies to en-
11 sure adequate progress, technological con-
12 sistency and policy compliance; and regu-
13 larly report the findings to Congress.

14 (B) CONTENT OF POLICIES, PROCEDURES,
15 GUIDELINES, RULES, AND STANDARDS.—The
16 policies, procedures, guidelines, rules, and
17 standards under subparagraph (A)(ii) shall—

18 (i) take into account the varying mis-
19 sions and security requirements of agencies
20 participating in the Environment;

21 (ii) address development, implementa-
22 tion, and oversight of technical standards
23 and requirements;

24 (iii) address and facilitate information
25 sharing between and among departments

1 and agencies of the intelligence community,
2 the Department of Defense, the Homeland
3 Security community and the law enforce-
4 ment community;

5 (iv) address and facilitate information
6 sharing between Federal departments and
7 agencies and State, tribal and local govern-
8 ments;

9 (v) address and facilitate, as appro-
10 priate, information sharing between Fed-
11 eral departments and agencies and the pri-
12 vate sector;

13 (vi) address and facilitate, as appro-
14 priate, information sharing between Fed-
15 eral departments and agencies with foreign
16 partners and allies; and

17 (vii) ensure the protection of privacy
18 and civil liberties.

19 (h) ESTABLISHMENT OF EXECUTIVE COUNCIL.—

20 There is established an Executive Council on Information
21 Sharing that shall assist the principal officer as designated
22 under subsection 206(g) in the execution of the duties
23 under this Act concerning information sharing.

24 (1) MEMBERSHIP.—The Executive Council shall
25 be chaired by the principal officer as designated in

1 subsection 206(g). The members of the Executive
2 Council shall be—

3 (A) the Director of Management and
4 Budget;

5 (B) the Secretary of Homeland Security or
6 his designee;

7 (C) the Secretary of Defense or his des-
8 ignee;

9 (D) the Attorney General or his designee;

10 (E) the Secretary of State or his designee;

11 (F) the Director of the Federal Bureau of
12 Investigation or his designee;

13 (G) the National Intelligence Director or
14 his designee;

15 (H) The Director of Central Intelligence
16 Agency or his designees;

17 (I) such other Federal officials as the
18 President shall designate;

19 (J) representatives of State, tribal, and
20 local governments, to be appointed by the Presi-
21 dent; and

22 (K) individuals who are employed in pri-
23 vate businesses or nonprofit organizations that
24 own or operate critical infrastructure, to be ap-
25 pointed by the President.

1 (2) RESPONSIBILITIES.—The Executive Council
2 shall assist the President in—

3 (A) implementing and managing the Envi-
4 ronment;

5 (B) developing policies, procedures, guide-
6 lines, rules, and standards necessary to estab-
7 lish and implement the Environment;

8 (C) ensuring there is coordination among
9 departments and agencies participating in the
10 Environment in the development and implemen-
11 tation of the Environment;

12 (D) reviewing, on an ongoing basis, poli-
13 cies, procedures, guidelines, rules, and stand-
14 ards related to the implementation of the Envi-
15 ronment;

16 (E) establishing a dispute resolution proc-
17 ess to resolve disagreements among depart-
18 ments and agencies about whether particular
19 information should be shared and in what man-
20 ner; and

21 (F) considering input provided by persons
22 from outside the Federal government with sig-
23 nificant experience and expertise in policy, tech-
24 nical, and operational matters, including issues
25 of security, privacy, or civil liberties.

1 (3) INAPPLICABILITY OF FEDERAL ADVISORY
2 COMMITTEE ACT.—The Council shall not be subject
3 to the requirements of the Federal Advisory Com-
4 mittee Act (5 U.S.C. App.).

5 (4) REPORTS.—Not later than 1 year after the
6 date of the enactment of this Act, and annually
7 thereafter, the principal officer as designated in sec-
8 tion 206(g), shall submit a report to the President
9 and to Congress that shall include—

10 (A) a description of the activities and ac-
11 complishments of the Council in the preceding
12 year; and

13 (B) the number and dates of the meetings
14 held by the Council and a list of attendees at
15 each meeting.

16 (5) INFORMING THE PUBLIC.—The Executive
17 Council shall—

18 (A) make its reports to Congress available
19 to the public to the greatest extent that is con-
20 sistent with the protection of classified informa-
21 tion and applicable law; and

22 (B) otherwise inform the public of its ac-
23 tivities, as appropriate and in a manner con-
24 sistent with the protection of classified informa-
25 tion and applicable law.

1 (i) REPORTS.—

2 (1) IN GENERAL.—Not later than 15 months
3 after the date of the enactment of this Act, and
4 semiannually thereafter, the President shall submit
5 a report to Congress on the state of the Environ-
6 ment and of information sharing across the Federal
7 government.

8 (2) CONTENT.—Each report under this sub-
9 section shall include—

10 (A) a progress report on the extent to
11 which the Environment has been implemented,
12 including how the Environment has fared on
13 the governmentwide and agency-specific per-
14 formance measures and whether the perform-
15 ance goals set in the preceding year have been
16 met;

17 (B) objective systemwide performance
18 goals for the following year;

19 (C) an accounting of how much was spent
20 on the Environment in the preceding year;

21 (D) actions taken to ensure that agencies
22 procure new technology that is consistent with
23 the Environment and information on whether
24 new systems and technology are consistent with
25 the Environment;

1 (E) the extent to which, in appropriate cir-
2 cumstances, all terrorism watch lists are avail-
3 able for combined searching in real time
4 through the Environment and whether there are
5 consistent standards for placing individuals on,
6 and removing individuals from, the watch lists,
7 including the availability of processes for cor-
8 recting errors;

9 (F) the extent to which unnecessary road-
10 blocks, impediments, or disincentives to infor-
11 mation sharing, including the inappropriate use
12 of paper-only intelligence products and require-
13 ments for originator approval, have been elimi-
14 nated;

15 (G) the extent to which positive incentives
16 for information sharing have been implemented;

17 (H) the extent to which classified informa-
18 tion is also made available through the Environ-
19 ment, in whole or in part, in unclassified form;

20 (I) the extent to which State, tribal, and
21 local officials—

22 (i) are participating in the Environ-
23 ment;

24 (ii) have systems which have become
25 integrated into the Environment;

1 (iii) are providing as well as receiving
2 information; and

3 (iv) are using the Environment to
4 communicate with each other;

5 (J) the extent to which—

6 (i) private sector data, including infor-
7 mation from owners and operators of crit-
8 ical infrastructure, is incorporated in the
9 Environment; and

10 (ii) the private sector is both pro-
11 viding and receiving information;

12 (K) where private sector data has been
13 used by the Government or has been incor-
14 porated into the Environment—

15 (i) the measures taken to protect sen-
16 sitive business information; and

17 (ii) where the data involves informa-
18 tion about individuals, the measures taken
19 to ensure the accuracy of such data;

20 (L) the measures taken by the Federal
21 government to ensure the accuracy of other in-
22 formation on the Environment and, in par-
23 ticular, the accuracy of information about indi-
24 viduals;

1 (M) an assessment of the Environment's
2 privacy and civil liberties protections, including
3 actions taken in the preceding year to imple-
4 ment or enforce privacy and civil liberties pro-
5 tections and a report of complaints received
6 about interference with an individual's privacy
7 or civil liberties; and

8 (N) an assessment of the security protec-
9 tions of the Environment.

10 (j) AGENCY RESPONSIBILITIES.—The head of each
11 department or agency possessing or using intelligence or
12 homeland security information or otherwise participating
13 in the Environment shall—

14 (1) ensure full department or agency compli-
15 ance with information sharing policies, procedures,
16 guidelines, rules, and standards established for the
17 Environment under subsections (c) and (g);

18 (2) ensure the provision of adequate resources
19 for systems and activities supporting operation of
20 and participation in the Environment; and

21 (3) ensure full agency or department coopera-
22 tion in the development of the Environment and as-
23 sociated enterprise architecture to implement gov-
24 ernmentwide information sharing, and in the man-

1 agement and acquisition of information technology
2 consistent with applicable law.

3 (k) AGENCY PLANS AND REPORTS.—Each Federal
4 department or agency that possesses or uses intelligence
5 and homeland security information, operates a system in
6 the Environment or otherwise participates, or expects to
7 participate, in the Environment, shall submit to the prin-
8 cipal officer as designated in section 206(g)—

9 (1) not later than 15 months after the date of
10 the enactment of this Act, a report including—

11 (A) a strategic plan for implementation of
12 the Environment's requirements within the de-
13 partment or agency;

14 (B) objective performance measures to as-
15 sess the progress and adequacy of the depart-
16 ment or agency's information sharing efforts;
17 and

18 (C) budgetary requirements to integrate
19 the agency into the Environment, including pro-
20 jected annual expenditures for each of the fol-
21 lowing 5 years following the submission of the
22 report; and

23 (2) annually thereafter, reports including—

24 (A) an assessment of the progress of the
25 department or agency in complying with the

1 Environment's requirements, including how well
2 the agency has performed on the objective
3 measures developed under paragraph (1)(B);

4 (B) the agency's expenditures to imple-
5 ment and comply with the Environment's re-
6 quirements in the preceding year; and

7 (C) the agency's or department's plans for
8 further implementation of the Environment in
9 the year following the submission of the report.

10 (l) PERIODIC ASSESSMENTS.—

11 (1) COMPTROLLER GENERAL.—

12 (A) IN GENERAL.—Not later than 15
13 months after the date of the enactment of this
14 Act, and periodically thereafter, the Comptroller
15 General shall evaluate the implementation of
16 the Environment, both generally and, at the
17 discretion of the Comptroller General, within
18 specific departments and agencies, to determine
19 the extent of compliance with the Environ-
20 ment's requirements and to assess the effective-
21 ness of the Environment in improving informa-
22 tion sharing and collaboration and in protecting
23 privacy and civil liberties, and shall report to
24 Congress on the findings of the Comptroller
25 General.

1 (B) INFORMATION AVAILABLE TO THE
2 COMPTROLLER GENERAL.—Upon request by the
3 Comptroller General, information relevant to an
4 evaluation under subsection (a) shall be made
5 available to the Comptroller General under sec-
6 tion 716 of title 31, United States Code.

7 (C) CONSULTATION WITH CONGRESSIONAL
8 COMMITTEES.—If a record is not made avail-
9 able to the Comptroller General within a rea-
10 sonable time, before the Comptroller General
11 files a report under section 716(b)(1) of title
12 31, United States Code, the Comptroller Gen-
13 eral shall consult with the Select Committee on
14 Intelligence of the Senate, the Permanent Se-
15 lect Committee on Intelligence of the House of
16 Representatives, the Committee on Govern-
17 mental Affairs of the Senate, and the Com-
18 mittee on Government Reform of the House of
19 Representatives concerning the Comptroller's
20 intent to file a report.

21 (2) INSPECTORS GENERAL.—The Inspector
22 General in any Federal department or agency that
23 possesses or uses intelligence or homeland security
24 information or that otherwise participates in the En-

1 vironment shall, at the discretion of the Inspector
2 General—

3 (A) conduct audits or investigations to—

4 (i) determine the compliance of that
5 department or agency with the Environ-
6 ment's requirements; and

7 (ii) assess the effectiveness of that de-
8 partment or agency in improving informa-
9 tion sharing and collaboration and in pro-
10 tecting privacy and civil liberties; and

11 (B) issue reports on such audits and inves-
12 tigations.

13 (m) AUTHORIZATION OF APPROPRIATIONS.—There
14 are authorized to be appropriated—

15 (1) \$50,000,000 to carry out this section for
16 fiscal year 2005; and

17 (2) such sums as are necessary to carry out this
18 section in each fiscal year thereafter, to be disbursed
19 and allocated in accordance with the Environment
20 implementation plan required by subsection (f).

21 **SEC. 207. ALTERNATIVE ANALYSES OF INTELLIGENCE BY**
22 **THE INTELLIGENCE COMMUNITY.**

23 (a) SENSE OF CONGRESS.—It is the sense of Con-
24 gress that the National Intelligence Director should con-
25 sider the advisability of establishing for each element of

1 the intelligence community an element, office, or compo-
2 nent whose purpose is the alternative analysis (commonly
3 referred to as a “red-team analysis”) of the information
4 and conclusions in the intelligence products of such ele-
5 ment of the intelligence community.

6 (b) REPORT.—(1) Not later than one year after the
7 date of the enactment of this Act, the National Intel-
8 ligence Director shall submit to Congress a report on the
9 actions taken to establish for each element of the intel-
10 ligence community an element, office, or component de-
11 scribed in subsection (a).

12 (2) The report shall be submitted in an unclassified
13 form, but may include a classified annex.

14 **SEC. 208. REPORT ON IMPLEMENTATION OF RECOMMENDA-**
15 **TIONS OF DEFENSE SCIENCE BOARD ON PRE-**
16 **VENTING AND DEFENDING AGAINST CLAN-**
17 **DESTINE NUCLEAR ATTACK.**

18 (a) FINDING.—Congress finds that the June 2004 re-
19 port of the Defense Science Board Task Force on Pre-
20 venting and Defending Against Clandestine Nuclear
21 Attack—

22 (1) found that it would be easy for adversaries
23 to introduce and detonate a nuclear explosive clan-
24 destinely in the United States;

Withdrawal Marker

The George W. Bush Library

3

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Email	Re: Info-Sharing Provisions of Collins-Lieberman Bill - To: David Sadoff	1	10/04/2004	P3/b3; P5; b7f; 50 USC 3507

**This marker identifies the original location of the withdrawn item listed above.
For a complete list of items withdrawn from this folder, see the
Withdrawal/Redaction Sheet at the front of the folder.**

COLLECTION:

National Security Council - Legal Adviser

SERIES:

Sadoff, David

FOLDER TITLE:

Information Sharing: Intelligence Reform Legislation

FRC ID:

35336

OA Num.:

NSC 1099

NARA Num.:

FOIA ID and Segment:

2017-0425-F

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

- A. Closed by Executive Order 13526 governing access to national security information.
- B. Closed by statute or by the agency which originated the document.
- C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Withdrawal Marker

The George W. Bush Library

4

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Email	Re: More... - To: David Sadoff	2	10/04/2004	P3/b3; P5; b7f; 50 USC 3507

**This marker identifies the original location of the withdrawn item listed above.
For a complete list of items withdrawn from this folder, see the
Withdrawal/Redaction Sheet at the front of the folder.**

COLLECTION:

National Security Council - Legal Adviser

SERIES:

Sadoff, David

FOLDER TITLE:

Information Sharing: Intelligence Reform Legislation

FRC ID:

35336

OA Num.:

NSC 1099

NARA Num.:

FOIA ID and Segment:

2017-0425-F

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advise between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

- A. Closed by Executive Order 13526 governing access to national security information.
- B. Closed by statute or by the agency which originated the document.
- C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Withdrawal Marker

The George W. Bush Library

5

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Letter	[Letter] - To: Susan M. Collins, et al - From: Thomas Ridge, et al	4	04/13/2004	P3/b3; P6/b6; b7c; b7f; 50 USC 3507

**This marker identifies the original location of the withdrawn item listed above.
For a complete list of items withdrawn from this folder, see the
Withdrawal/Redaction Sheet at the front of the folder.**

COLLECTION:

National Security Council - Legal Adviser

SERIES:

Sadoff, David

FOLDER TITLE:

Information Sharing: Intelligence Reform Legislation

FRC ID:

35336

OA Num.:

NSC 1099

NARA Num.:

FOIA ID and Segment:

2017-0425-F

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

Freedom of Information Act - [5 U.S.C. 552(b)]

P1 National Security Classified Information [(a)(1) of the PRA]

P2 Relating to the appointment to Federal office [(a)(2) of the PRA]

P3 Release would violate a Federal statute [(a)(3) of the PRA]

P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]

P5 Release would disclose confidential advise between the President and his advisors, or between such advisors [(a)(5) of the PRA]

P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

A. Closed by Executive Order 13526 governing access to national security information.

B. Closed by statute or by the agency which originated the document.

C. Closed in accordance with restrictions contained in donor's deed of gift.

b(1) National security classified information [(b)(1) of the FOIA]

b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]

b(3) Release would violate a Federal statute [(b)(3) of the FOIA]

b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]

b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]

b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]

b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]

b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

Withdrawal Marker

The George W. Bush Library

6

FORM	SUBJECT/TITLE	PAGES	DATE	RESTRICTION(S)
Draft	Memorandum	7	N.D.	P5;

**This marker identifies the original location of the withdrawn item listed above.
For a complete list of items withdrawn from this folder, see the
Withdrawal/Redaction Sheet at the front of the folder.**

COLLECTION:

National Security Council - Legal Adviser

SERIES:

Sadoff, David

FOLDER TITLE:

Information Sharing: Intelligence Reform Legislation

FRC ID:

35336

OA Num.:

NSC 1099

NARA Num.:

FOIA ID and Segment:

2017-0425-F

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advise between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

Deed of Gift Restrictions

- A. Closed by Executive Order 13526 governing access to national security information.
- B. Closed by statute or by the agency which originated the document.
- C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]