ORAL ARGUMENT NOT SCHEDULED

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 12-5158

PUBLIC EMPLOYEES FOR ENVIRONMENTAL RESPONSIBILITY, Appellant,

v.

U.S. SECTION, INT'L BOUNDARY AND WATER COMMISSION, U.S. - MEXICO, Appellee.

BRIEF FOR APPELLEE

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

RONALD C. MACHEN JR.,
United States Attorney.

R. CRAIG LAWRENCE,
JANE M. LYONS,
Assistant United States Attorneys.

C.A. No. 11-261

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Parties

Appellant, plaintiff below, is Public Employees for Environmental Responsibility.

Appellee, defendant below, is the U.S. Section of the International Boundary and Water Commission between the United States and Mexico, which is part of the United States Department of Homeland Security. There are no intervenors or *amicus curiae*.

Ruling Under Review

At issue is the Honorable Barbara J. Rothstein's March 21, 2012 Order Granting Defendant's Motion for Summary Judgment and Denying Plaintiff's Cross Motion for Summary Judgment. The decision appears at pages 7-42 of the Joint Appendix filed on January 22, 2013.

Related Cases

This case has not previously been before this Court. Undersigned counsel is not aware of any related cases.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

(*Cases chiefly relied upon are marked with asterisks*)

Federal Cases

Federal Statutes

Federal Rules

Miscellaneous

STATUTORY PROVISION - 5 U.S.C. § 552

(a)(3)(C) In responding under this paragraph to a request for records, an agency shall make reasonable efforts to search for the records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency's automated information system.

(D) For purposes of this paragraph, the term "search" means to review, manually or by automated means, agency records for the purpose of locating those records which are responsive to a request.

(b) This section does not apply to matters that are—

. . .

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

. . .

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information

. . .

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or

(F) could reasonably be expected to endanger the life or physical safety of any individual;

. . .

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. The amount of information deleted, and the exemption under which the deletion is made, shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made. If technically feasible, the amount of the information deleted, and the exemption under which the deletion is made, shall be indicated at the place in the record where such deletion is made.

GLOSSARY OF ABBREVIATIONS

DHS ..... Department of Homeland Security

FOIA ..... Freedom of Information Act

IBWC ..... International Boundary and Water Commission

NIPP ..... National Infrastructure Protection Plan

PEER ..... Public Employees for Environmental Responsibility

USACE ..... United States Army Corps of Engineers

USBR ..... United States Bureau of Reclamation

U.S. Section ..... U.S. Section of Int'l Boundary & Water Comm'n Between the United States and Mexico

JURISDICTIONAL STATEMENT

The District Court had jurisdiction over the Freedom of Information Act claims under 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1331. This Court has jurisdiction under 28 U.S.C. § 1291 because PEER filed a timely notice of appeal of the March 21, 2012 Order under review. *See* Fed. R. App. P. 4(a)(1)(B).

STATEMENT OF ISSUES

In the opinion of Appellee, the following issues are presented:

1. Whether the District Court properly found that the U.S. Section had conducted a reasonable search for responsive records and released all reasonably segregable, non-exempt information, and that PEER had failed to show any genuine issue of material fact.
2. Whether the U.S. Section properly withheld a Joint Expert Report under Exemption 5 because it contains pre-decisional, deliberative material relating to the U.S. Section's ongoing role in protecting property along the Rio Grande River, and the outside consultants who worked on the report had neither advocacy nor self-interests in the U.S. Section's policymaking.
3. Whether the U.S. Section satisfied the threshold for asserting Exemption 7 for withholding emergency action plans and inundation maps by showing that those records or information were compiled for law enforcement purposes based on the U.S. Section's role working with the Department of

Homeland Security to protect dams as part of the National Infrastructure Protection Plan.

4. Whether the U.S. Section's withholding of guidelines for law enforcement within the emergency action plans for Amistad and Falcon Dams and power plants was appropriate under Section 7(E) because disclosure could reasonably be expected to risk circumvention of the law by those who might seek to disrupt or interfere with the safe operation of the dams or first responders in the event of an emergency.
5. Whether the U.S. Section correctly withheld inundation maps under Exemption 7(F) of the FOIA because their release could reasonably be expected to endanger lives or physical safety of people living proximate to the dams or levees by facilitating more damaging attacks on the dams or levees.

COUNTERSTATEMENT OF THE CASE

PEER filed this action on January 31, 2011 to challenge the U.S. Section's response to its Freedom of Information Act request dated August 10, 2010. JA 1, 43. On April 11, 2011, the U.S. Section moved for summary judgment. On May 16, 2011, PEER opposed the U.S. Section's motion and cross-moved for summary judgment. On June 17, 2011, the U.S. Section filed its reply and opposition to PEER's motion for summary judgment. Finally, PEER filed its reply on June 29,

2011. The next day, the U.S. Section filed an erratum correcting two of the declarations it had previously submitted by including language making them subject to penalty of perjury. JA 165-75.

On March 21, 2012, the District Court granted the U.S. Section's motion for summary judgment and denied PEER's cross-motion. JA 7-42. PEER filed a timely notice of appeal on May 17, 2012. *See* JA 19.

COUNTERSTATEMENT OF FACTS

I. The International Boundary and Water Commission and the U.S. Section

By way of general background and according to information on its website, the International Boundary and Water Commission, U.S. - Mexico

> traces its roots to the 1848 Treaty of Guadalupe Hidalgo and the Gadsden Treaty of 1853, which established temporary joint commissions to survey, map, and demarcate with ground landmarks the new United States (U.S.) and Mexico boundary. . . .
>
> The U.S. and Mexico established the International Boundary Commission (IBC) on March 1, 1889 as another temporary body to apply the rules that were adopted by the Convention of 1884. The IBC was extended indefinitely in 1900 and is considered the direct predecessor to the modern day International Boundary and Water Commission. . .
>
> The IBC was instrumental in developing the second water distribution treaty between the United States and Mexico in 1944, which addressed utilization of the waters of the Colorado River and Rio Grande from Fort Quitman, Texas to the Gulf of Mexico. The Water Treaty of February 3, 1944 expanded the duties and responsibilities of the IBC and renamed it the International Boundary and Water Commission (IBWC). The 1944 Treaty charged the IBWC

> with the application of the treaty and the exercise of the rights and obligations which the U.S. and Mexican Governments assumed thereunder and with the settlement of all disputes that were to arise under the treaty. . . .
>
> Pursuant to the 1944 treaty the IBWC has the status of an international body and consists of a United States Section and a Mexican Section. Each Section is headed by an Engineer Commissioner. Wherever there are provisions for joint action or joint agreement between the two Governments or for the furnishing of reports, studies, or plans to the two Governments, it is understood that those matters will be handled by or through the Department of State of the United States and the Ministry of Foreign Relations of Mexico. Each Government affords diplomatic status to the Commissioner, designated by the other Government. The Commission, its two principal engineers, a legal advisor, and a secretary, designated by each Government as members of its Section of the Commission are entitled in the territory of the other country to the privileges and immunity appertaining to diplomatic officers. . . .

"History of the International Boundary and Water Commission" (available at ibwc.state.gov/About_Us/history.html); *see also* 22 U.S.C. §§ 277d-34, 277d-41, 277d-3 & 277d-16 (authorizing appropriations to the State Department for the U.S. Section); 22 U.S.C. § 277d-7 (authorizing appropriations directly to the U.S. Section). The U.S. Section of the Commission ("U.S. Section") is also "a member agency of the Interagency Committee on Dam Safety[], established by the National Dam Safety Act, 33 U.S.C. § 467 *et seq*." JA 55.

"The Interagency Committee on Dam Safety works in conjunction with the Office of Infrastructure Protection within the Department of Homeland Security (DHS) which serves as the Sector-Specific Agency for the Dams Section of the

National Infrastructure Protection Plan (NIPP)." *Id.* The mission of the Interagency Committee on Dam Safety, which is part of the Department of Homeland Security, is to "encourage the establishment and maintenance of effective Federal programs, policies, and guidelines intended to enhance dam safety for the protection of human life and property through coordination and information exchange among Federal agencies concerning implementation of the Federal Guidelines for Dam Safety." *See* 33 U.S.C. § 467e; JA 68-69.

Because it is an establishment in the Executive branch, the U.S. Section is subject to the FOIA. *See* 22 U.S.C. § 277; 33 U.S.C. § 467e; 5 U.S.C. § 552(f)(1).

II. PEER's FOIA Request and the U.S. Section's Responses

PEER sent a Freedom of Information Act, 5 U.S.C. § 552 ("FOIA") request dated August 10, 2010 to the U.S. Section requesting information about eight records or categories of records. JA 43-45; *see* JA 70. Generally, PEER sought information about the U.S. Section's activities relating to Amistad Dam, Falcon Dam, and the Presidio levee, as well as "demolition and/or reconstruction of any levees located in or adjacent to Canutillo and Mesilla." *Id.* PEER requested technical reports, emergency action plans, e-mails and other documents. *Id.*

In response to PEER's request, the U.S. Section conducted a manual search for records in its Safety of Dams Section within its Operations and Maintenance Division. *See* JA 57. Using an employee possessing "significant experience

regarding the reports and other technical documents pertaining to the Amistad Dam, Falcon Dam and Presidio level" to assist with the search, the U.S. Section initially located multiple records responsive to some but not all of the items PEER requested. *See* JA 57-59. By letter dated September 28, 2010, the U.S. Section initially responded to PEER's request by indicating, for each itemized category of records from the request, whether responsive records had been located and, if so, whether they were being released in whole or in part. JA 46-47. The U.S. Section also notified PEER that it was withholding certain draft documents under Exemption 5 of the FOIA and the deliberative process privilege. *Id*.

PEER administratively appealed portions of the U.S. Section's response on October 15, 2010. *See* JA 48-51. In particular, PEER challenged the U.S. Section's assertion that it had been unable to locate "the November 2009 report issued by a panel of technical advisers regarding the condition of Amistad Dam and plan of action" and e-mails relating to that report. JA 49-50. Additionally, PEER objected to application of Exemption 5 to records responsive to its request for "current inundation maps and emergency action plans for areas downstream of Falcon Dam and Amistad Dam." JA 50. PEER's administrative appeal also suggested that even if Exemtion 5 applied, that the inundation maps and emergency action plans being withheld might at least contain reasonably segregable non-exempt information. *See* JA 50-51.

By letter dated November 29, 2010, the U.S. Section released some additional information to PEER based on information provided for the first time in PEER's administrative appeal which had enabled the U.S. Section to locate a report dated in October, 2009. *See* JA 53, 59-60. But the U.S. Section noted that it was withholding it under Exemption 2 "specifically because disclosure of such information could facilitate illegal acts against critical infrastructure." JA 53. The U.S. Section further stated that it had located a correspondence relating to the October, 2009 report and was releasing some and withholding some as pre-decisional material. *See* JA 53-54. With respect to inundation maps, the U.S. Section indicated that it had "located one binder containing 77 drafts of 77 inundation maps" which it was withholding under Exemptions 2 and 5 "as pre-decisional, deliberative process documents, and . . . [because] disclosure of such information could facilitate illegal acts against critical infrastructure." JA 54. Further, the U.S. Section released two documents responsive to PEER's request for emergency action plans with certain material withheld under Exemptions 2 and 6. *Id.* And finally, the U.S. Section's appeal response letter advised PEER of its right to seek judicial review. *Id.* PEER did just that.

III. This Litigation and the District Court's Decision

On January 31, 2011, PEER filed a complaint in the District Court challenging the U.S. Section's response to its FOIA request. *See* JA 1, 4-6. The

complaint included violations of the FOIA as well as the Administrative Procedure Act. *See* JA 11-12; R.1. On March 7, 2011, the Supreme Court held in *Milner v. Dep't of Navy*, 131 S. Ct. 1259 (2011), that the language in Exemption 2 of the FOIA should be read more literally than lower courts had been applying it. *Id*. at 1264-66.

The parties subsequently cross-moved for summary judgment. *See* JA 1-2, 68-73 (U.S. Section's Statement of Material Facts), 78-83 (PEER's Statement of Material Facts); JA 103-04 (U.S. Section's Response to PEER's Statement of Material Facts); JA 99-102 (U.S. Section's Reply to PEER's narrative response to U.S. Section's Statement of Material Facts).[1] Consistent with advancing its own cross-motion for summary judgment at the outset, PEER did not request any discovery. But PEER did attempt to challenge the legitimacy of the U.S. Section's assertion that the dams and levees it sought information about were the subject of some concern as possible targets for terrorists or others seeking to disrupt homeland security. *See* JA 91-93. PEER characterized an April, 2010 communication about Falcon Dam from the Department of Homeland Security to the U.S. Section as a "false warning," a "hoax," and "an entirely fictional terrorist plot." JA 91. For support, PEER pointed exclusively to "numerous news accounts

[1] PEER's response to the U.S. Section's Statement of Material Facts is not in the Joint Appendix and may be found in the District Court's docket at R.8, pages 9-25 of 41.

that officials said at the time there was no credible evidence of a threat" against Falcon Dam *Id.*

Notably, in light of the Supreme Court's then-recent decision in *Milner*, the U.S. Section re-reviewed its response to PEER's FOIA request and by the time it moved for summary judgment, the U.S. Section had entirely abandoned its reliance on Exemption 2. JA 69. In its summary judgment motion in the District Court, the U.S. Section asserted Exemptions 5, 6, 7(E) and (F). JA 57-62, *see* JA 71-73. Importantly, the U.S. Section provided evidence of dams as potential targets for terrorist attacks generally and confirmed its receipt of the particular notice it had received from the Department of Homeland security less than four months before PEER requested records. *See* JA 55, 56; *see also* JA 99-100 (describing system for classifying dams and stating that both Amistad and Falcon Dam are classified as "high-hazard dams").

On March 21, 2012, the District Court granted the U.S. Sections' motion and denied PEER's. JA 7-42. In an opinion thoroughly addressing the evidence and the arguments raised by both parties, the District Court ultimately dismissed PEER's APA claim (JA 18), found that the U.S. Section had conducted a reasonable search in light of PEER's FOIA request and appeal, rejected PEER's suggestion that the U.S. Commission had responded to its FOIA request in less

than good faith, and upheld the U.S. Commission's applications of Exemptions 5, 6, 7(E) and (F). JA 18-39.

Further, the District Court found that the U.S. Section had demonstrated sufficiently that all reasonably segregable non-exempt material had been released and that the record did not justify a written finding under 5 U.S.C. § 552(a)(4)(F)(i) referring agency personnel to the Office of Special Counsel for possible disciplinary action for arbitrarily mishandling the response to PEER's FOIA request. JA 40-42. On the latter point, the District Court noted that the record actually contained "some evidence to suggest . . . that the [U.S. Section] handled PEER's FOIA request in exactly the same manner as it has handled requests from other parties." JA 42. The District Court also denied PEER's request for attorney's fees because PEER had not substantially prevailed. JA 41.

This appeal followed.

SUMMARY OF ARGUMENT

This case lies at the intersection of public disclosure under FOIA and public safety. As pertinent to this case, working through the Interagency Commission on Dam Safety and with the Department of Homeland Security, the U.S. Section contributes to the mission to protect the nation's borders and to secure critical infrastructure, including dams, from potential threats.

The District Court correctly granted summary judgment in favor of the U.S. Section. The record demonstrates that the U.S. Section conducted a reasonable search for responsive records subject to the FOIA and released all reasonably segregable non-exempt information. Not only are PEER's accusations of bad faith in responding to the FOIA request unfounded, they are also contradicted by a record of the U.S. Section's attentiveness and voluntary expansion of its search during the administrative appeal phase as well as its prompt release of 1,492 pages of material prior to litigation.

The District Court also properly recognized that a Joint Expert Report about Amistad Dam is exempt from disclosure under the deliberative process privilege, made applicable through 5 U.S.C. § 552(b)(5), because its disclosure would reveal internal agency deliberations. The participation of consultants from outside the U.S. Section in the project that produced the Joint Report does not take the Joint Report outside of the deliberative process privilege because the outsiders lacked any conflict of interest in the U.S. Section's evaluation. Much as the consultants in *McKinley v. Bd. of Governors of Fed. Reserve*, 647 F.3d 331 (D.C. Cir. 2011), *cert. denied*, 132 S. Ct. 1026 (2012), had the shared goal of studying potential financial infirmities of a major player in the financial market, the representatives from Mexico here shared the common goal of ensuring the safety of a dam on the border between the U.S. and Mexico. The Joint Report is also deliberative

because it was commissioned to inform the U.S. Section about measuring the potential risks to the structural integrity of Amistad Dam and its classification rating. And the factual material contained within the Joint Report could not be reasonably released without revealing what the experts considered as important to the question. Preserving the ability of technical experts to provide judgment for the benefit of the U.S. Section and the public without fear of having it revealed is appropriate to encourage those experts to be candid and forthcoming.

The District Court also correctly determined that the records concerning dam safety and classification were compiled for law enforcement purposes in the course of the U.S. Section's work with law enforcement charged with protecting public safety and securing key elements of infrastructure as part of the National Infrastructure Protection Plan. Further, the law enforcement guidelines within the emergency action plans for Amistad and Falcon dams are exempt under Exemption 7(E) from disclosure because their release would unacceptably risk circumvention of the law by increasing the chance of either an attack or undermining law enforcement's response to an attack. And the inundation maps fall under Exemption 7(F) because their release could reasonably be expected to endanger life or physical safety of people living downstream from these two dams in the event of an emergency.

STANDARD OF REVIEW

This Court's review of the merits of summary judgment is *de novo*. *American Civil Liberties Union v. U.S. Dep't of Justice*, 655 F.3d 1, 5 (D.C. Cir. 2011). This review is limited, absent exceptional circumstances, insofar as the Court reviews only arguments made in the District Court. *See Potter v. District of Columbia*, 558 F.3d 542, 547, 550 (D.C. Cir. 2009).

ARGUMENT

I. The Record Affirmatively Demonstrates the U.S. Section's Good Faith In Responding to PEER's Request and Releasing All Reasonably Segregable Non-Exempt Records Covered By FOIA.

A. The Record Demonstrates the U.S. Section's Good Faith

Although PEER does not appear to challenge the adequacy of the U.S. Section's search by the time it filed this case in the District Court, it does contend that the U.S. Section's initial failure to locate the technical report PEER described in its FOIA request as a "November 2009 report" demonstrated bad faith. Appellant's Br. at 11-14. PEER further accuses the U.S. Section of misconduct during litigation. *Id*. These arguments lacks merit both as a matter of law and of fact.

Courts practically and properly evaluate the agency's response at the time they resolve motions for summary judgment, and not at some earlier point in the process, such as the exhaustion of a FOIA claim administratively or the filing of

the complaint in district court. *See Tijerina v. Walters*, 821 F.2d 789, 799 (D.C. Cir. 1987) ("'[H]owever fitful or delayed the release of information under FOIA may be . . . if we are convinced appellees have, however belatedly, released all nonexempt material, we have no further judicial function to perform under the FOIA.'") (quoting *Perry v. Block*, 684 F.2d 121, 125 (D.C. Cir. 1982)). *See also Ground Saucer Watch, Inc. v. CIA*, 692 F.2d 770, 772 (D.C. Cir. 1981) ("Indeed, if the release of previously withheld materials were held to constitute evidence of present 'bad faith,' similar evidence would exist in every FOIA case involving additional releases of documents after the filing of suit.").

In this case, the U.S. Section's recognition during the administrative appeal phase that the report PEER had requested might not have been issued in November, 2009 as PEER indicated in its request but, rather, sometime around November, 2009, is an example of why the courts should focus at summary judgment on the agency's final response, and not some interim point. *See* JA 56-60. The purpose of the mandatory exhaustion procedure was well served in this case precisely because, during the administrative appeal phase, the U.S. Section re-examined its initial response and expanded its search parameters sufficiently to locate the report PEER was seeking. And that is evidence of the U.S. Section's good faith. JA 53, 59; *Meeropol v. Meese*, 790 F.2d 942, 953 (D.C. Cir. 1986) (disclosure indicates good-faith, law-abiding behavior); *see Itturalde v.*

Comptroller of Currency, 315 F.3d 311, 315 (D.C. Cir. 2003) (holding that bad faith is not indicated by "initial delays in responding to a FOIA request."). Further, the reasonableness of the search is tied to the request itself, and the discrepancy between the date in the FOIA request as written (which was limited to "the November, 2009 report" (JA 43), as opposed to, for example, "a report issued between September and December, 2009") and the actual date of the report (October, 2009) demonstrates the reasonableness of the U.S. Section's initial search. *Meeropol*, 790 F.2d at 956; *see Miller v. Casey*, 730 F.2d 773, 776-77 (D.C. Cir. 1984) (affirming summary judgment and noting that agencies must read and interpret a FOIA request as it was drafted, "not as either [an] agency official or [the requester] might wish it was drafted."). Thus, PEER's arguments fail legally both because they focus incorrectly on the initial instead of the total search and improperly ignore the role of an inaccuracy in PEER's own request in assessing the adequacy of the search.

Additionally, PEER's other accusations of bad faith are directly and amply contradicted by undisputed evidence in the record that the U.S. Section's initial search in response to the seven other categories of records listed in PEER's FOIA request resulted in the identification and release of 1,492 pages of material. *See* JA 71. PEER's suggestion of bad faith ignores the undisputed fact that so much

material was promptly identified and released in response to other parts of its FOIA request.

B. PEER's Arguments Fail To Show Any Error in the District Court's Analysis

PEER's various arguments fail to demonstrate any error by the District Court. First, PEER's assertion that the U.S. Section denied having a FOIA office at some point is of no moment because it is undisputed that the U.S. Section promptly provided PEER nearly 1,500 pages of material in September 2010, thoroughly adjudicated PEER's administrative appeal, including by identifying and/or releasing additional material. *See* Brief For Appellant at 6-7. Likewise, PEER's request that the Court take judicial notice of the fact that the U.S. Section ignored their FOIA request in another instance (Brief for Appellant at 15) is unwarranted because the U.S. Section has amply responded to the FOIA request at issue in this case and responded to claims in this litigation.[2] Ultimately, whatever misinformation PEER claims to have received at an early stage of the administrative process here or hard feelings concerning some other FOIA request are insufficient to create a genuine issue of material fact in this case. The Court,

[2] Additionally, PEER failed to demonstrate that judicial notice is appropriate under Fed. R. Evid. 201. Because PEER sought to attribute mal-intent to the past fact of litigation between the same parties, judicial notice would have been inappropriate.

therefore, should affirm the grant of summary judgment in the U.S. Section's favor.[3]

Similarly, PEER's contention that the first Fitten declaration was insufficient (Brief for Appellant at 15) rings hollow because PEER correctly notes that the U.S. Section submitted a second Fitten declaration which was executed "under penalty of perjury," (*Id*. at 16 n.7), and the law is settled that the declarant in a FOIA case need not have personal knowledge. The applicable standard here allows agencies to rely on declarations by people, such as Mr. Fitten, who supervise the search even if they did not personally conduct it. *Meeropol*, 790 F.2d at 951. The Fitten declarations satisfy that standard, and PEER has failed to identify any systems of records reasonably likely to contain responsive records that the U.S. Section should have looked in and failed to do so. Accordingly, the District Court's finding that the search was reasonable should be affirmed. *Truitt v. Dep't of State*, 897 F.2d 540, 542 (D.C. Cir. 1990); *Perry v. Block*, 684 F.2d 121, 126-27 (D.C. Cir. 1982).

[3] Even were the Court to conclude on this record that some sort of bad faith had been shown, the appropriate remedy would be reversing summary judgment and remanding to the District Court for further development of the record, not granting summary judgment in PEER's favor. *E.g., Morley v. CIA*, 508 F.3d 1108, 1121 (D.C. Cir. 2007) (instructing the district court that "[o]n remand the CIA must supplement its explanation"); *Campbell v. U.S. Dep't of Justice*, 164 F.3d 20, 37 (D.C. Cir. 1998) (remanding to the district court so it could order the agency to conduct a more adequate search).

Finally, PEER's arguments that (1) the U.S. Section had "greatly exaggerated" the notice from the Department of Homeland Security of a possible credible threat to Falcon Dam (JA 170-71); and (2) that the Federal Emergency Management Agency ("FEMA") or other agencies require or encourage sharing emergency plans to assist downstream communities in preparing their own emergency response plans emergency action plans do not alter the analysis under FOIA. Appellant's Br. at 22, 24-26. First, neither the Government's evaluation of the credibility of an isolated threat nor the means of assessing it is typically reported in newspapers and PEER fails to identify any official statements by federal officials dismissing the Intelligence Alert concerning Falcon Dam (JA 167-68, 170) as a hoax. PEER fails to create a genuine issue of material fact because news articles contain hearsay which is generally inadmissible at summary judgment. *See Gleklen v. Democratic Cong. Campaign Comm., Inc.*, 199 F.3d 1365, 1369 (D.C. Cir. 2000).

Even if the Government ultimately decided that the particular threat lacked credibility, however, the U.S. Section mentioned but does not rely heavily on that Intelligence Alert to establish that its records were compiled for law enforcement purposes. In that sense, PEER's treatment of the April 2010 Intelligence Report is a red herring. By far the more critical and indisputable fact is that the large dams PEER inquired about are identified as part of the National Infrastructure

Protection Plan mandated by the President. *See generally* Addendum 3 (identifying dams as one of the critical infrastructure sectors). Working with the Department of Homeland Security, the U.S. Section is responsible for assisting with developing policies and guidelines on dam safety to protect these critical parts of the nation's infrastructure from possible terrorist or other threats and planning for contingencies in the event of emergencies. With respect to the areas PEER's FOIA request implicates, there is a close nexus between the U.S. Section and parts of the Department of Homeland Security responsible for law enforcement, including dam safety and border protection. Because the National Infrastructure Protection Plan designates these dams as high risk, the Court should be loath to second-guess the Executive Branch's contemporaneous or ongoing assessment of either a potential terrorist attack or the need to restrict access to information for particular structures or facilities. *E.g.*, *Ameziane v. Obama*, 699 F.3d 488, 494 (D.C. Cir. 2012).

Second, PEER has failed to proffer evidence of FEMA releasing publicly any information comparable to that which PEER seeks here. Because release under the FOIA is a release to the world (*National Archives & Records Admin. v. Favish*, 541 U.S. 157, 170-71 (2004)), PEER's observation (bordering on speculation) that FEMA encourages release of information generally regarding dam safety or emergency action plans should not vitiate the U.S. Section's ability

to withhold the particular records sought here under FOIA because each agency has the discretion to exercise and FEMA's actions do not bind the U.S. Section. *See* Appellant's Br. at 14. California law (Appellant's Br. at 27) is not binding on the U.S. Section. PEER failed to show that any of the particular records they requested from the U.S. Section have been disclosed to any members of the public. The possible availability of similar records involving other dams in California or relating to dams classified as lower risks is unpersusasive as a reason to make the U.S. Section's records public because the comparison is inapt. *See Afshar v. Department of State*, 702 F.2d 1125, 1130 (D.C. Cir. 1983) (noting that "official acknowledgment by an authoritative source" of a fact that "is the subject of widespread media and public speculation" may "be new information that could cause damage to the national security"). And although the records are not classified, the U.S. Section has justified them as sufficiently sensitive that a level of deference by the Court, but lower than would be afforded classified information, is appropriate because the records relate to national security and the possible actual threat and planning for possible attacks in the United States on structures with the potential to cause harm to people downstream from Amistad Dam. *See Ameziane v. Obama*, 699 F.3d at 494-95 (holding that Government entitled to a protective order covering Task Force transfer decisions and all related or derivative documents concerning prisoners held at Guantanamo Bay).

C. The District Court Correctly Found that the U.S. Section Had Released All Reasonably Segregable Non-Exempt Information

FOIA requires that, if a record contains information that is exempt, any "reasonably segregable" information must be disclosed after deletion of the exempt information unless the non-exempt portions are "inextricably intertwined with exempt portions." 5 U.S.C. § 552(b); *Hodge v. Federal Bureau of Investigation*, 703 F.3d 575, 580 (D.C. Cir. 2013); *Mead Data Central, Inc. v. U.S. Dep't of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977). To demonstrate that all reasonably segregable material has been released, the agency must provide a "detailed justification" rather than "conclusory statements." *Mead Data*, 566 F.2d at 261. The agency is not, however, obliged "to provide such a detailed justification" that the exempt material would effectively be disclosed. *Id*. All that is required is that the government show "with 'reasonable specificity'" why a document cannot be further segregated. *Armstrong v. Executive Office of the President*, 97 F.3d 575, 578-79 (D.C. Cir. 1996). Importantly, the agency is not required to "commit significant time and resources to the separation of disjointed words, phrases, or even sentences which taken separately or together have minimal or no information content." *Mead Data*, 566 F.2d at 261, n.55.

In evaluating whether the U.S. Section has satisfied the requirement of segregating non-exempt material from exempt material, this Court has found that an agency is "entitled to a presumption that [it] complied with the obligation to

disclose reasonably segregable material." *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1117 (D.C. Cir. 2007) (cited with approval in *Hodge*, 703 F.3d at 580). The District Court's decision did not explicitly rely on a presumption; instead the District Court affirmatively found that the record demonstrated that the U.S. Section has "discharged its burden of showing with reasonable specificity why documents could not be further segregated." JA 40.

PEER attempts to overcome the presumption only with respect to the U.S. Section's withholdings under Exemption 5 by claiming that the Fitten Declaration was too conclusory. *See* Appellant's Br. at 38-39. Ironically, PEER's own argument in this regard is rather conclusory. *Id*. The first Fitten Declaration explains that the U.S. Section released 12 of 13 e-mails and documents relating to the Joint Expert Report, and describes the one that was withheld. JA 60. Logically, the release of 12 out of 13 responsive records demonstrates that the agency carefully evaluated each record individually. Further, the Fitten Declaration described in reasonable detail the one withheld e-mail and its relationship to "legal or policy-related dam safety matters," and affirmatively states that the records were examined to ensure that non-exempt portions not "inextricably intertwined with exempt portions" had been released. JA 60-62. PEER's thin speculation that the records might have additional portions that could be released without amounting to gibberish is insufficient to rebut either the

presumption or the evidence that the U.S. Section has provided all reasonably segregable information. *E.g.*, *Hodge*, 575 F.3d at 580 (affirming district court's finding on segregablility without *in camera review* when plaintiff proffered records he argued showed that records produced in the same case suggested that additional non-exempt material could have been released).

To the extent PEER would rely on evidence relating to the initial processing or search, or its uninformed opinion or speculation that the U.S. Section either over-reacted to or was supposedly duped by a terrorism threat lacking credibility, PEER cites no cases, and we are aware of none, finding that the segregability determination at the end of the processing stage is called into any question by events earlier in the case. *Cf. Juarez v. Department of Justice*, 518 F.3d 54, 60 (D.C. Cir. 2008) (remand for segregability analysis by the District Court was unnecessary where the Court had the same record before it and its review was *de novo* and the task was to assess the legal sufficiency of the agency's grounds for withholding under the FOIA). The Court should, therefore, affirm the District Court's finding that the U.S. Section released all reasonably segregable non-exempt information.

II. The U.S. Section Properly Applied Exemptions 5 and 7 to Certain Information and Records

FOIA places the burden of justifying that the requested material withheld falls within one of its exemptions on the agencies subject to the FOIA. 5 U.S.C. §

552(a)(4)(B); *see Petroleum Info. Corp. v. Dep't of Interior*, 976 F.2d 1429, 1433 (D.C. Cir. 1992). This Court has described that burden as a "substantial" one, *Morley v. Central Intelligence Agency*, 508 F.3d at 1114, but the Supreme Court has also observed that "[w]hen disclosure touches upon certain areas defined in the exemptions . . .[,] the [FOIA] recognizes limitations that compete with the general interest in disclosure, and that, in appropriate cases, can overcome it." *Nat'l Archives & Records Admin.*, 541 U.S. at 172.

To meet their burden, agencies typically provide courts with declaration(s) and a *Vaughn*[4] index describing their application of exemptions available under FOIA. *See Judicial Watch, Inc. v. FDA*, 449 F.3d 141, 146 (D.C. Cir. 2006). To prevail, this evidence must provide a "relatively detailed justification" justifying the agency's actions. *Mead Data Ctr., Inc. v. U.S. Dep't of Air Force*, 566 F.2d at 251; *see Judicial Watch*, 449 F.3d at 146-147; *King v. U.S. Dep't of Justice*, 830 F.2d 210, 219 (D.C. Cir. 1987).

In this case, the U.S. Section asserted Exemptions 5, 6, and 7, and the District Court upheld the U.S. Section's reliance on those exemptions in their entirety. JA 23-39; *see* JA 76. This brief will not address the withholdings under Exemption 6 because PEER does not challenge the U.S. Section's assertion of Exemption 6 over private contact information (JA 76) in its opening brief. *Board*

[4] *Vaughn v. Rosen*, 523 F.2d 1136 (D.C. Cir. 1975).

of Regents of Univ. of Wash. v. EPA, 86 F.3d 1214, 1221 (D.C. Cir. 1996) (holding that "issues not raised until the reply brief are waived").

A. The U.S. Section Properly Withheld the Joint Expert Report Under Exemption 5

1. Exemption 5

Exemption 5 of the FOIA protects "interagency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." 5 U.S.C. § 552(b)(5). To be covered by Exemption 5, a document's "source must be a Government agency, and it must fall within the ambit of a privilege against discovery under judicial standards that would govern litigation against the agency that holds it." *Department of the Interior v. Klamath Water Users Protection Ass'n*, 532 U.S. 1, 8-9 (2001). In other words, "the parameters of Exemption 5 are determined by reference to the protections available to litigants in civil discovery; if material is not 'available' in discovery, it may be withheld from FOIA requesters." *Burka v. Dep't of Health & Human Servs.*, 87 F.3d 508, 516 (D.C. Cir. 1996); *see also Williams & Connolly v. Securities & Exchange Comm'n*, 662 F.3d 1240, 1243 (D.C. Cir. 2011).

2. Exemption 5 and the Deliberative Process Privilege Cover the Joint Expert Report Commissioned by the U.S. Section

In this case, the U.S. Section applied Exemption 5 in conjunction with the deliberative process privilege to withhold an email dated November 13, 2009[5] and a Joint Expert Panel Review of the Amistad Dam because they reflecting internal agency deliberations. JA 76; *Sears, Roebuck & Co.*, 421 U.S. 132, 150 (1975); *Wolfe v. Dep't of Health & Human Servs.*, 839 F.2d 768, 774 (D.C. Cir. 1988) (en banc). In assessing the applicability of the deliberative process privilege, "the

[5] Because PEER limits is argument in its opening brief to the Joint Report and fails to develop an argument challenging the withholding of the November 13, 2009 e-mail, PEER should be deemed to have waived any issue regarding the e-mail. *City of Waukesha v. Environmental Protection Agency*, 320 F.3d 228, 250 n.22 (D.C. Cir. 2003) (per curiam) (argument inadequately raised in opening brief is waived). As a result, the Court should affirm the U.S. Section's withholding of the November 13, 2009 e-mail. If the Court were to address it, the e-mail is "predecisional correspondence reflecting a deliberative process involved in the finalization of the report." JA 60. The *Vaughn* index reflects that the author of the e-mail was Tony Solo, that Mr. Solo sent the e-mail to four individuals, and that the subject was "Comments on Interim Risk Reduction Measures, EAP review." JA 76. The record also contains a declaration from Luis Hernandez, one of the recipients of the November 13, 2009 e-mail (JA 107), who describes himself as a civil engineer employed by the U.S. Section. *Id*. Although the other three recipients are not specifically identified as employees of the U.S. Section or another Government agency, PEER assigns no error to the District Court's finding that this e-mail "is an internal communication between agency employees regarding deliberations and comments as to interim risk reduction measures." JA 23; *See* Appellant's Br. at 32-36. The date of the e-mail being after the October, 2009 report relating to the same subject is not dispositive because the record makes clear that the U.S. Section continued to assess and consider policy relating to Amistad Dam without adopting or referenceing the e-mail. *See Brennan Ctr. for Justice at New York Univ. School of Law v. U.S. Dep't of Justice*, 697 F.3d 184 (2d Cir. 2012).

primary question is whether disclosure of the materials would expose an agency's decision-making process in a way that could discourage candid discussion within the agency and thereby undermine the agency's ability to perform its functions." *See Formaldehyde Inst. v. Dep't of Health & Human Servs.*, 889 F.2d 1118, 1122 (D.C. Cir. 1989), *overruled on other grounds by Nat'l Inst. of Military Justice v. Dep't of Defense*, 512 F.3d 677 (D.C. Cir. 2008). To be deliberative, the findings need to reflect the "give-and-take" or "consultative process." *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980); *see Judicial Watch, Inc. v. FDA*, 449 F.3d at 151.

With respect to the Joint Report, PEER contends that Exemption 5 is inapplicable because non-agency employees contributed to the Joint Report and because the U.S. Section failed to show that the Joint Report was part of a deliberative process. Appellant's Br. at 32-36. As to the former, the participation of people outside of the U.S. Section does not vitiate Exemption 5 because both the Supreme Court and this Court have recognized the "consultant corollary" that allows agencies to protect agency records containing comments solicited from those outside the agency without a clear conflict of interest in the government's

decision.[6] *Klamath*, 532 U.S. at 11; *National Inst. of Military Justice.*, 512 F.3d at 680.

The "consultant corollary" doctrine applies here much the same way it did in *McKinley v. Bd. of Governors of Fed. Reserve*, 647 F.3d 331, 333 (D.C. Cir. 2011), when the Court held that Exemption 5 applied to allow withholding of certain records relating to the Board of Governors of the Federal Reserve's investigation of possible financial infirmities of a major market player. *Id*. at 333, 336-39. In *McKinley*, this Court found that the Board and member Reserve Banks "share a common goal, namely 'the maintenance of a sound and orderly financial system.'" *Id*. at 337. Here, the U.S. Section and CONAGUA (the Mexican National Water Commission) share the common goal of ensuring the safety of the dams. Thus, the result should be the same here as in *McKinley*.

On the other hand, this case is unlike *Dep't of Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1 (2001), because CONAGUA has no

[6] With regard to the Joint Report, the *Vaughn* index reflects authorship exclusively by the U.S. Army Corps of Engineers and the U.S. Bureau of Reclamation. JA 76. The Statement of Facts PEER filed in the District Court included a footnote (JA 81) quoting language from the U.S. Section's website stating that the U.S. Section had "selected and convened a panel of highly qualified 'expert' consultants to work under the guidance of the agency's Technical Advisors (USACE and CONAGUA) . . ." *Id*. Because this language appears to relate to the Joint Report and this issue does not alter the analysis or the outcome, the U.S. Section is not arguing, for purposes of this appeal, about the role of the agency's technical advisors. Were this case to be remanded for any reason, however, the U.S. Section reserves the right to supplement the record to clarify the role of Technical Advisors on the project.

discernible self-interest in dam safety that diverges from the U.S. Section's. The Joint Report concerns safety and the nature of the U.S. Section's mission as part of the International Boundary and Water Commission makes it especially appropriate for it to solicit the views of experts on the Mexican side of the border because the U.S. Section's function includes furthering harmonious interaction between the U.S. and Mexico on issues touching their common border. *See also Hunton & Williams v. U.S. Dep't of Justice*, 590 F.3d 272 (4th Cir. 2010) (applying Exemption 5 to communications by DOJ with outside attorneys for a telecommunications firm under a common interest theory). PEER proffer no evidence that the outside consultants from CONAGUA had any sort of self-advocacy interests or were seeking any benefits. And nothing PEER has proffered demonstrates any policy change or commercial or financial transaction flowing from the Joint Report. Consequently, *Klamath* is inapposite, and a different result is warranted.

The District Court also found that the context of the Joint Report established its deliberative quality, and rejected PEER's attack on it. JA 23-27, 28-29; *see* Appellant's Br. at 34-36. "The deliberative process privilege rests on the obvious realization that officials will not communicate candidly among themselves if each remark is a potential item of discovery and front page news, and its object is to enhance the quality of agency decisions by protecting open and

frank discussion among those who make them within the Government." *Klamath*, 532 U.S. at 8-9 (internal quotations and citation omitted).

The key undisputed facts here are that the U.S. Section solicited the Joint Report as part of its ongoing responsibility to consider possible risks to the structural integrity of Amistad Dam and its classification rating as part of the U.S. Section's fulfillment of its function as a member of the Interagency Committee on Dam Safety. *See* JA 59-60. More specifically, the Joint Report provides the U.S. Section "considerations about the types of metrics that the [U.S. Section] might consider key in its continued examination of deficiencies, strengths, adequacies, and projections." JA 60. Thus, it is apparent that the Joint Report contains deliberative material associated with the U.S. Section's ongoing activities relating to protecting property along the Rio Grande from floods. *Id*. Nothing about the Joint Report suggests that it contains any policy or "working law." *See Public Citizen, Inc. v. Office of Mgmt. & Budget*, 598 F.3d 865, 875 (D.C. Cir. 2010). Nor does the law require the U.S. Section to pinpoint a particular final decision that the Joint Report was part of or to which it contributed or was considered. *Sears*, 421 U.S. at 151 n.18 (extending Exemption 5 protection to records that are part of the decisionmaking process even where the process does not produce an actual decision by the agency); s*ee Wolfe v. HHS*, 839 F.2d at 775-76 (the status of an agency decision within the agency's decisionmaking process may be

protective when the release of information would have the effect of prematurely disclosing "the recommended outcome of the consultative process"). Thus, disclosure of the Joint Report could reasonably harm the U.S. Section by exposing recommendations or analysis never finally adopted by the agency.

Indeed, disclosure of the recommendations and internal impressions in the Joint Report could also reasonably be expected to chill or to discourage candor in communications. The U.S. Section issues official reports (some of which are available on its website at http://www.ibwc.state.gov/EMD/reports_studies.html), and the fact that this Joint Report is not one of them reflects that the joint authors lack legal decision-making authority for the agency, a factor that favors of protection under Exemption 5. *Schlefer v. U.S.*, 702 F.2d 233, 238-39 (D.C. Cir. 1983). Further, the evidence PEER proffers (Appellant's Br. at 36) to support the notion that the U.S. Section intends to adopt some, but not all, of the recommendations in the Joint Report even more clearly demonstrates the pre-decisional nature of the Joint Report at the time it was prepared and continuing to the present. And that the Joint Report is being considered by people with the power to adopt, implement, or reject recommendations shows that it is part of a deliberative process, and this is an area where "there should be considerable deference to the [agency's] judgment as to what constitutes. . . 'part of the agency give-and-take - of the deliberative process. *See Vaughn* 523 F.2d at 1144. Thus,

the District Court correctly found that both required elements of the test for deliberative process are satisfied here. JA 28-29.

Finally, PEER argues that factual material in the Joint Report is not covered by the deliberative process privilege and should have been released. *See* Appellant's Br. at 36-39. Although purely factual material ordinarily must be segregated out and released, *Coastal States*, 617 F.2d at 867, this Court has also recognized that the distinction is not universally simple and declared that factual information should be examined "in light of the policies and goals that underlie" the privilege and in "the context in which the materials are used." *Wolfe*, 839 F.2d at 774; *Nat'l Wildlife Fed'n v. U.S. Forest Serv.*, 861 F.2d 1114, 1119 (9th Cir. 1988) (emphasizing that the "ultimate objective" of Exemption 5 is to safeguard the agency's deliberative process). For the Joint Report, the assemblage of facts and their presentation appears itself to have been a product of discretion and judgment for the benefit of policy-makers within the U.S. Section. *See* JA 59 ("report prepared by panel of experts and consultants to assist the USIBWC in its evaluation of the greatest potential risks in the Amistad Dam's foundation and embankment . . . also provided the USIBWC with recommendations about the Dam's safety rating. The objective of the Joint Panel Review Report of the Amistad Dam was . . . specifically to assist the USIBWC in its deliberations with the Amistad's Dam Safety Classification rating currently used by the Corps of

Engineers (COE)"). This material should be protected under this Court's decisions in *Mapother v. DOJ*, 3 F.3d 1533 (D. C. Cir. 1993), and *Montrose Chem. Corp. v. Train*, 491 F.2d 63 (D.C. Cir. 1974), because its distillation and screening of facts from the existing technical facts about the Amistad Dam (which was constructed in 1969) represents an exercise of judgment for the benefit of people at the U.S. Section called upon to make policy. JA 59.

So long as the Court accepts the application of the deliberative process to the Joint Report, it need go no further on this issue.[7] Because the Joint Report was the product of experts convened "to assess the structural condition of the Amistad Dam, and to make recommendations with regard to the dam's safety rating" as required by the Dam Safety Act, the Court should affirm withholding the Joint Report under Exemption 5.

[7] Although PEER hints in its Statement of Issues (Appellant's Br. at 3) that the U.S. Section failed to show "what specific harm to the decision-making process would result from disclosure" of the Joint Report, PEER fails to develop that argument in the body of its brief. *See* Fed. R. App. P. 28(a)(9)(A) (argument requires "the appellant's contentions and the reasons for them, with citations to the authorities and parts of the record on which the appellant relies"). Tacking on a phrase in a multi-level statement of issues alone fails to constitute argument because the contention through suggestion lacks both analysis and pertinent citations. *See, e.g., Greater New Orleans Fair Housing Action Ctr. v. HUD*, 639 F.3d 1078, 1091 (D.C. Cir. 2011); *Chalabi v. Hashemite Kingdom of Jordan*, 543 F.3d 725, 730 (D.C. Cir. 2008). In any event, the party's need for information covered by the deliberative process privilege is not a factor considered under the FOIA. *North v. Walsh*, 881 F.2d 1088, 1096 (D.C. Cir. 1989) ("In sum, [FOIA requester's] need or intended use for the documents is irrelevant.").

B. The Record Demonstrates That the U.S. Section Satisfies the Exemption 7 Threshold

The U.S. Section withheld inundation maps and emergency action plans ("EAPs") under Exemption 7. *See* JA 76. All of these records were prepared by the U.S. Army Corps of Engineers (identified as "USACE" on the *Vaughn*; *see* JA 108) and the U.S. Bureau of Reclamation (identified as "USBR" on the *Vaughn*) for the U.S. Section. *See* JA 60-62.

Before invoking any specific sub-section of Exemption 7, agencies are required to demonstrate that "the records or information [were] compiled for law enforcement purposes." 5 U.S.C. § 552(b)(7). In this context, the term "law enforcement purposes extends beyond the criminal and into the civil realm. *See North v. Walsh*, 881 F.2d 1088, 1098 (D. C. Cir. 1989) (stating that the 1986 amendment of FOIA "changed the threshold requirement for withholding information under exemption 7" so that "it now applies more broadly); *Tax Analysts*, 294 F.3d 71, 79 (D.C. Cir. 2002) (explaining that the legislative history of the 1986 amendment shows that it was intended "to protect investigatory and non-investigatory materials"); *Mittleman v. OPM*, 76 F.3d 1240, 1243 (D.C. Cir. 1996). Even if information was not initially obtained or generated for law enforcement purposes, it can still qualify under Exemption 7 if it was subsequently compiled for a valid law enforcement purpose prior to the assertion of Exemption 7. *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 153 (1989).

The "law" to be enforced within the phrase "law enforcement purposes" includes civil and criminal statutes, as well as statutes authorizing administrative proceedings. *Rural Hous. Alliance v. USDA*, 498 F.2d 73, 81 & n.46 (D.C. Cir. 1974), *opinion supplemented*, 511 F.2d 1347 (D.C. Cir. 1974); *see Jefferson v. Dep't of Justice*, 284 F.3d 172, 178 (D.C. Cir. 2002). More recently, this Court has also recognized that "law enforcement" within the meaning of Exemption 7 can extend beyond traditional realms into realms of national security and homeland security-related government activities. *Ctr. For Nat'l Sec. Studies v. DOJ*, 331 F.3d 918, 926, 929 (D.C. Cir. 2003) (holding that names of post-9/11 detainees could be withheld based on the needs of homeland security even though the Government would ordinarily make such information publicly available), *cert. denied*, 540 U.S. 1104 (2004). All of these principles apply here.

The Homeland Security Act of 2002 provides the principle statutory authority for Department of Homeland Security's responsibilities in the protection of critical infrastructure. That statute assigns DHS the responsibility for developing a comprehensive national plan for securing critical infrastructure and for recommending the "measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government

agencies and authorities, the private sector, and other entities." 6 U.S.C. § 121(d)(6).

The President outlined the national approach for critical infrastructure protection in Homeland Security Presidential Directive 7 (HSPD-7) which was revised and reissued on February 12, 2013 as Presidential Policy Directive 21 (PPD-21). The directive establish the U.S. policy for enhancing protection of critical infrastructure, identifies the main categories of critical infrastructure (called "Sectors"), and directs DHS to develop, and subsequently update, a national plan to accomplish the President's goals and objectives. In accordance with these Presidential policy documents, and as directed by the Homeland Security Act, DHS issued the National Infrastructure Protection Plan ("NIPP") in 2006 and a revision in 2009. Among other things, the NIPP delineates the roles and responsibilities for federal agencies, and other partners, in carrying out critical infrastructure protection activities while respecting and integrating the authorities, jurisdictions, and prerogatives of these partners.

The President, in HSPD-7 and PPD-21, specifically designated dams as a critical infrastructure sector, bringing the government agencies and owner operators in the dam sector under the organizational structures outlined in the

NIPP.[8] The NIPP, to accomplish public-private coordination within sectors, establishes public and private sector bodies composed of representatives from within the sector. Government departments, agencies, and programs with equities in the dam sector make up the Dams Government Coordinating Council, which is responsible for coordinating strategies, activities, policy, and communications across the sector. The U.S. Section is a member of the Dam Government Coordinating Council (Addendum 22), establishing it as a formal member of the NIPP Framework and the national critical infrastructure protection mission.

Consequently, the U.S. Section comfortably satisfied the threshold for Exemption 7 under *Ctr. For Nat'l Sec. Studies* by "establish[ing] (1) a rational nexus between the investigation and one of the agency's law enforcement duties; and (2) a connection between an individual or incident and a possible security risk or violation of federal law." *Ctr. For Nat'l Sec. Studies*, 331 F.3d at 926 (internal quotation and citations omitted). The District Court found that the U.S. Section had shown the nexus between the inundation maps and emergency action plans and law enforcement duties. JA 35, citing *Ctr. For National Sec. Studies*, 331 F.3d at 926. That is plainly correct because "[t]he maps reveal populated areas at risk should the downstream areas become flooded by a breach of the Amistad Dam" as well as "estimated travel times for flood progression, . . . peak elevation

[8] Copies of HSPD-7 and PPD-21, as well as the Dams Sector Government Coordinating Council Charter are appended to this brief.

of [flood] waters." JA 61. They were created "to assist emergency management officials such as the sheriff's deputies in the most affected counties . . . as well as the local office of the Federal Bureau of Investigation and US Border Patrol." *Id.*

Likewise, the emergency action plans (which were withheld only in part), contain similar inundation data, including "descriptions of surveillance plans, logistics, and conclusions meant for interagency use in case of an emergency caused by a failure of either the Falcon or Amistad Dams." JA 62. As such, these records are tightly connected to and associated with the U.S. Section's statutory responsibilities as part of the Interagency Committee on Dam Safety which itself has law enforcement responsibilities by virtue of its role in protecting public safety. *See* 33 U.S.C. §§ 467e, 467f. These materials are the product of investigation of possible terrorist attacks and classification of dams. In its role working with DHS, the U.S. Section furthers law enforcement by providing technical assistance either to assist with preventing or responding to public safety emergencies. *Cf.* 6 U.S.C. § 121(d); *see also* 42 U.S.C. § 5195c(e) (defining the term "critical infrastructure"); 18 U.S.C. § 2339D.

Consequently, the District Court's finding that the U.S. Section possesses a sufficient nexus to law enforcement should be affirmed. Additionally, although there may have been multiple reasons for compiling the information PEER seeks relating to certain dams, because those dams are also part of the critical

infrastructure, one of those purposes is to be available for safety, security, protection against terrorist acts, and recovery.

C. The Guidelines for Law Enforcement Contained in the Emergency Action Plans Fall Under Exemption 7(E)

1. Exemption 7(E)

Exemption 7(E) of the FOIA protects all information compiled for law enforcement purposes when its release "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). This Court "sets a relatively low bar for the agency to justify withholding" information under Exemption 7(E)." *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011). The exemption allows for withholding information in the face of "not just for circumvention of the law, but for a risk of circumvention; not just for an actual or certain risk of circumvention, but for an expected risk; not just for an undeniably or universally expected risk, but for a reasonably expected risk; and not just for certitude of a reasonably expected risk, but for the chance of a reasonably expected risk." *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1193 (D.C. Cir. 2009).

2. The U.S. Section Cleared the "Relatively Low Bar" for Withholding Law Enforcement Guidelines

The U.S. Section applied Exemption 7(E) to withhold various guidelines for law enforcement that are part of the Emergency Action Plans for the Amistad and Falcon Dams and power plants. JA 76. The record reflects that these include "descriptions of surveillance plans, logistics and conclusions meant for interagency use in case of an emergency caused by failure of either the Falcon or Amistad Dams." JA 62. The U.S. Section further explained the disclosure of "such sensitive information risks circumvention of the law by those who might seek to exact the greatest amount of damage against the public affected by a dam failure or flood event." *Id*. All of this information falls under Exemption 7(E) because the record substantiates that Falcon and Amistad dams are considered possible terrorist targets because of the potential for mass casualties associated with dam failure or impairment. JA 55. The record here also contains specific evidence of an April, 2010 Intelligence Alert concerning reports that drug traffickers were planning to blow up Falcon Dam. JA 158.

Courts have specifically applied Exemption 7(E) to protect from disclosure guidelines for safeguarding resources as well as security procedures. *Whitfield v. U.S. Dep't of Treasury*, 255 Fed. App'x. 533 (D.C. Cir. 2007) (affirming withholding of details of arrest procedures because they could assist suspects seeking to evade arrest); *Williams v. Dep't of Justice*, 171 Fed. App'x. 857 (D.C.

Cir. 2005) (upholding bank security techniques involving use of bait money under Exemption 7(E); *see generally Mayer Brown LLP v. IRS*, 562 F.3d at 1192-93 (discussing the meaning of the phrase "could be expected to risk circumvention of the law" found in Exemption 7(E)). PEER's challenge to the U.S. Section's reliance on Exemption 7(E) is based on the sufficiency of proof "that the claimed enumerated harms are present." Appellant's Br. at 28. But that argument misses the mark because the burden of the U.S. Section is only to show the risk of harms, and not the harms themselves. The government's plans for responding to an emergency at one of the dams would be of obvious utility to anyone planning to disrupt operations at a dam who could neutralize or compromise the effectiveness of those emergency response plans by circumventing protections or exploiting vulnerabilities. Because the risk is self-evident and PEER's reliance on newpaper reports fails to create a genuine issue of material fact on the existence of a risk, Exemption 7(E) protects the material in the EAPs from disclosure.

D. The Inundation Maps Are Exempt from Disclosure Because Their Release Could Reasonably Be Expected to Endanger the Life or Physical Safety of Any Individual

1. Exemption 7(F)

Exemption 7(F) permits agencies to withhold "records or information compiled for law enforcement purposes, but only to the extent that the production of such . . . records . . . could reasonably be expected to endanger the life or

physical safety of any individual." 5 U.S.C. § 552(b)(7)(F). It is axiomatic that the plain meaning of a statute controls its interpretation. *Performance Coal Co. v. Federal Mine & Health Review Com'n*, 642 F.3d 234, 240 (D.C. Cir. 2011) (finding a statutory provision "a model of near-perfect clarity"). In extending protection where disclosure "could reasonably be expected to endanger the life or physical safety of any individual[,]" the text of Exemption 7(F) does not limit its protection to some individuals at the exclusion of others or require precise identification. Because there is no logical reason to interpret the statute otherwise, the term "'any' . . . means any[.]" *Ford v. Mabus*, 629 F.3d 198, 206 (D.C. Cir. 2010), citing *United States v. Gonzales*, 520 U.S. 1, 5 (1997) (explaining that "any" has an "expansive meaning" and holding that because "Congress did not add any language limiting the breadth of that word" courts could not impose a limit).

The statutory history of Exemption 7(F) confirms this understanding. In its original form, Exemption 7(F) applied only to documents whose disclosure would "endanger the life of physical safety of any law enforcement officer." *See* 5 U.S.C. § 552(b)(7) (1982). In 1986, however, Congress expanded the exemption to encompass the life and physical safety "of any individual." Under familiar interpretive principles, the Court should give meaningful effect to that amendment. *Stone v. INS*, 514 U.S. 386, 397 (1995).

Consistent with its plain language, most courts that have addressed the issue have held that Exemption 7(F) encompasses any unspecified individual whose life or safety could reasonably be endangered by a disclosure. *But see American Civil Liberties Union v. Dep't of Defense*, 543 F.3d 59 (2d Cir. 2006) *cert. granted & vacated*, 130 S. Ct. 777 (2009). For example, in *Living Rivers, Inc. v. U.S. Bureau of Reclamation*, 272 F. Supp. 2d 1313, 1314 (D. Utah 2003), the Government invoked Exemption 7(F) in response to a request for copies of inundation maps for the areas below the Hoover and Glen Canyon Dams. Just like in this appeal, the maps at issue in *Living Rivers* assessed the potential effects of dam failure on downstream communities and power plants. *Id*. at 1315. According to the Bureau of Reclamation in that case, the maps presented a "worst-case scenario ... thus making the dam a more attractive target to [a potential] terrorist," and thereby risking "the life or physical safety of those individuals who occupy the downstream areas." *Id*. at 1316, 1321.

The court upheld the Government's reliance on Exemption 7(F). Describing the breadth of Exemption 7(F), the court reasoned that "Exemption 7(F) is neither limited to protect the lives of 'law enforcement personnel,' nor to known, named individuals only." *Id*. at 1321. The court also stressed that "[i]n evaluating the validity of an agency's invocation of Exemption 7(F), the court should 'within limits', defer to the agency's assessment of danger." *Id*. at 1321

(citation omitted). Applying that deference to the agency's risk assessment, the court held that the Bureau had properly withheld the maps pursuant to Exemption 7(F). *Id*. at 1322. *See Zadvydas v. Davis*, 533 U.S. 678, 696 (2001) (noting that "terrorism or other special circumstances" might warrant "heightened deference to the judgments of the political branches"); *Dep't of the Navy v. Egan*, 484 U.S. 518, 530 (1988) ("courts traditionally have been reluctant to intrude upon the authority of the executive in military and national security affairs").

Both the Supreme Court and this Court have explicitly endorsed appropriate deference to the executive in the context of FOIA claims which implicate national security. *See CIA v. Sims*, 471 U.S. 159, 179 (1985) ("The decisions of the Director [of Central Intelligence], who must of course be familiar with 'the whole picture,' as judges are not, are worthy of great deference given the magnitude of the national security interests and potential risks at stake"). And other courts in this district have applied Exemption 7(F) after finding a reasonable risk of violence against a broad range of unspecified individuals. For example, in *Center for Nat'l Security Studies v. United States Dep't of Justice*, 215 F. Supp. 2d 94, 108 (D.D.C. 2002), *aff'd in part and rev'd in part on other grounds*, 331 F.3d 918 (D.C. Cir. 2003), Exemption 7(F) was applied to the locations of detention facilities holding individuals connected to the terrorism investigation after September 11, 2001. The district court reasoned that disclosure would make the

facilities "vulnerable to retaliatory attacks, and 'place at risk not only [ ] detainees, but the facilities themselves and their employees.'" *Id.*

Likewise, in *Los Angeles Times Communications, LLC v. Department of the Army*, the court held that Exemption 7(F) protected from release information contained in Serious Incident Reports ("SIRs") submitted to the Army by private security contractors in Iraq. 442 F. Supp. 2d 880 (C.D. Cal. 2006). Notwithstanding plaintiffs' claim that the identity of private security contractors was a matter of great public interest, the court concluded that the names of the contractors in the SIRs were protected from release because that information, taken with other information, "may provide [insurgents] with enough information to organize attacks on vulnerable [private security contractor] companies or the projects they protect." *Id*. at 889-900.

In reaching that conclusion, the court accepted the "predictive judgments" of Army personnel that the disclosure of the company names "might very well be expected to endanger the life or safety of military personnel, [private security contractor] employees, and civilians in Iraq." *Id*. at 889. The court noted in that regard that "'the judiciary owes some measure of deference to the executive in cases implicating national security, a uniquely executive purview.' " *Id*. at 899 (quoting *Center for Nat'l Security Studies*, 331 F.3d at 926-27). Thus, the court concluded that:

> The test was not whether the court personally agrees in full with the [agency's] evaluation of the danger--rather, the issue is whether on the whole record the Agency's judgment objectively survives the test of reasonableness, good faith, specificity, and plausibility in this field of foreign intelligence in which the Agency is expert and given by Congress a special role.

Los Angeles Times Communications, 442 F.Supp.2d at 899 (quoting *Gardels v. CIA*, 689 F.2d 1100, 1105 (D.C. Cir. 1982) (citations omitted) (brackets in original)).

2. The U.S. Section Established That Release of the Inundation Maps Could Reasonably Be Expected to Endanger the Lives or Physical Safety of People Living Downstream

In addition to the decision in *Living Rivers*, the dam failure inundation maps in this case are comparable to some of the material addressed in *Milner*, where Justice Alito commented in his concurring opinion that the Navy

> has a fair argument that the Explosive Safety Quantity Distance (ESQD) information falls within Exemption 7(F). The ESQD information, the Navy argues, is used "for the purpose of identifying and addressing security issues" and for the "protection of people and property on the base, as well as in [the] nearby community, from the damage, loss, death, or injury that could occur from an accident or breach of security. . . . If, indeed, the ESQD information was compiled as part of an effort to prevent crimes of terrorism and to maintain security, there is a reasonable argument that the information has been "compiled for law enforcement purposes." § 552(b)(7). Assuming that this threshold requirement is satisfied, the ESQD information may fall comfortably within Exemption 7(F).

Milner, 131 S. Ct. at 1273 (Alito, J., concurring); *but see ACLU v. Dep't of Defense*, 543 F.3d 59, 82 (2d Cir. 2008) (denying withholding under Exemption

7(F) for photographs of detainees when the government articulated the danger as being from terrorism potentially directed at, among other groups, the populations of Iraq and Afghanistan, as well as members, employees and contractors of the U.S. military serving in those two countries), *cert. granted, vacated & remanded on other grounds*, 130 S. Ct. 777 (2009).

Although this Court does not appear to have addressed in any reported decision the degree of specificity necessary under Exemption 7(F) for identifying a person who could reasonably be expected to be endangered by disclosure of the information sought, PEER urges the Court to adopt the Second Circuit's rationale in *American Civil Liberties Union v. Dep't of Defense*, 543 F.3d 59 (2d Cir. 2008). Appellant's Br. at 30. In *ACLU*, the Second Circuit addressed a FOIA request for photographs of alleged prisoner abuse by U.S. military members in Iraq and Afghanistan. *Id*. at 63. Addressing an argument "raised as an afterthought" in the district court (*id*. at 66), the Second Circuit found that, despite its flexibility, Exemption 7(F)'s term "any individual" does not encompass "members of a group so large that risks which are clearly speculative for any particular individuals become reasonably foreseeable for the group." *Id*. at 67. In that case, the risk of harm to physical safety or life of members of the U.S. military, its contractors, coalition forces, and civilians in Iraq and Afghanistan failed. *Id*. at 71. Significantly, the Second Circuit made no effort "to shape the

precise contours" of Exemption 7(F) in *ACLU* because it found that it did not need to do so. *Id*. at 71.

The U.S. Section urges the Court to reject the Second Circuit's reading of "any individual" as flawed. It places excessive emphasis on the term "individual" to the point of virtually ignoring the preceding term "any." In any event, this case is also distinguishable from *ACLU* because the downstream residents (of the U.S. or Mexico) who would be devastated in the event of a dam failure represent a much smaller and more identifiable group than the entire populations of Iraq and Afghanistan during the U.S. military operations in those countries.

The more persuasive reasoning applied in a context much more similar to this case is found in *Living Rivers, Inc. v. Bureau of Reclamation*, 272 F. Supp. 2d 1313 (D. Utah). Although no more binding on this Court than *ACLU*, *Living Rivers* upheld the withholding of inundation maps under Exemption 7(F). *Id*. at 1321. Additionally, interpereting "any individual" not to require identification of a particular named person is consistent with this Court's interpretation of the same term in other statutes.

PEER's narrow reading of the term "any individual" in Exemption 7(F) to require identification of at least one actual person could reduce the analysis to whether the Government included in its declaration a name pulled at random out of voter registration rolls, motor vehicle registration records, or a telephone

directory of a town proximate to the Amistad Dam. The applicability of Exemption 7(F) should not turn on such artificialities because the U.S. Section has shown that release could reasonably be expected to danger life or physical safety of a group of people whom the parties agree exist.

CONCLUSION

WHEREFORE, for the foregoing reasons, Appellee respectfully requests that this Court affirm the District Court's judgment.

RONALD C. MACHEN JR.
United States Attorney

R. CRAIG LAWRENCE
Assistant United States Attorney

By: */s/ Jane M. Lyons*
JANE M. LYONS
Assistant United States Attorney
555 Fourth Street, N.W. – Civil Division
Washington, D.C. 20530
(202) 514-7161

Attorneys for Appellee

Dated: March 28, 2013

CERTIFICATE OF COMPLIANCE
FRAP 32(a)(7)(C)

The text for this Brief for Appellee is prepared using Times New Roman, 14 point and -- including the Statement of Issues but omitting those items described in Fed. R. App. P. 32(a)(7)(B)(iii) and D.C. Circuit Rule 32(a)(1) -- contains 11,752 words as counted by Microsoft Word 2010.

/s/ Jane M. Lyons
JANE M. LYONS
Assistant United States Attorney

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 28th day of March, 2013, I caused a true and correct copy of the above Brief for Appellee to be served upon Appellant's counsel through the Court's CM/ECF system.

/s/ Jane M. Lyons
JANE M. LYONS
Assistant United States Attorney
Civil Division
555 4th Street, N.W. – Room E4816
Washington, D.C. 20530
(202) 514-7161

For Immediate Release
Office of the Press Secretary
December 17, 2003

December 17, 2003 Homeland Security Presidential Directive/Hspd-7

Subject: Critical Infrastructure Identification, Prioritization, and Protection

Purpose

(1) This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

Background

(2) Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence.

(3) America's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. The majority of these are owned and operated by the private sector and State or local governments. These critical infrastructures and key resources are both physical and cyber-based and span all sectors of the economy.

(4) Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.

(5) While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.

Definitions

(6) In this directive:

(a) The term "critical infrastructure" has the meaning given to that

term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C.

5195c(e)).

(b) The term "key resources" has the meaning given that term in section 2(9) of the Homeland Security Act of 2002 (6 U.S.C. 101(9)).

(c) The term "the Department" means the Department of Homeland Security.

(d) The term "Federal departments and agencies" means those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.

(e) The terms "State," and "local government," when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(f) The term "the Secretary" means the Secretary of Homeland Security.

(g) The term "Sector-Specific Agency" means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category. Sector-Specific Agencies will conduct their activities under this directive in accordance with guidance provided by the Secretary.

(h) The terms "protect" and "secure" mean reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks.

Policy

(7) It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:

(a) cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;

(b) impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;

(c) undermine State and local government capacities to maintain order and to deliver minimum essential public services;

(d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;

(e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or

(f) undermine the public's morale and confidence in our national economic and political institutions.

(8) Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective.

(9) Federal departments and agencies will ensure that homeland security programs do not diminish the overall economic security of the United States.

(10) Federal departments and agencies will appropriately protect information associated with carrying out this directive, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

(11) Federal departments and agencies shall implement this directive in a manner consistent with applicable provisions of law, including those protecting the rights of United States persons.

Roles and Responsibilities of the Secretary

(12) In carrying out the functions assigned in the Homeland Security Act of 2002, the Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources. (13) Consistent with this directive, the Secretary will identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction.

(14) The Secretary will establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities.

(15) The Secretary shall coordinate protection activities for each of the following critical infrastructure sectors: information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping. The Department shall coordinate with appropriate departments and agencies to ensure the protection of other key resources including dams, government facilities, and commercial facilities. In addition, in its role as overall cross-sector coordinator, the Department shall also evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time, as appropriate.

(16) The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations. To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. The organization will support the Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law.

(17) The Secretary will work closely with other Federal departments and agencies, State and local governments, and the private sector in accomplishing the objectives of this directive.

Roles and Responsibilities of Sector-Specific Federal Agencies

(18) Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, there are designated Sector-Specific Agencies, including:

(a) Department of Agriculture -- agriculture, food (meat, poultry, egg products);

(b) Health and Human Services -- public health, healthcare, and food (other than meat, poultry, egg products);

(c) Environmental Protection Agency -- drinking water and water treatment systems;

(d) Department of Energy -- energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities;

(e) Department of the Treasury -- banking and finance;

(f) Department of the Interior -- national monuments and icons; and

(g) Department of Defense -- defense industrial base.

(19) In accordance with guidance provided by the Secretary, Sector-Specific Agencies shall:

(a) collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;

(b) conduct or facilitate vulnerability assessments of the sector; and

(c) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

(20) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance.

(21) Federal departments and agencies shall cooperate with the Department in implementing this directive, consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

Roles and Responsibilities of Other Departments, Agencies, and Offices

(22) In addition to the responsibilities given the Department and Sector-Specific Agencies, there are special functions of various Federal departments and agencies and components of the Executive Office of the President related to critical infrastructure and key resources protection.

(a) The Department of State, in conjunction with the Department, and the Departments of Justice, Commerce, Defense, the Treasury and other appropriate agencies, will work with foreign countries and international organizations to strengthen the protection of United States critical infrastructure and key resources.

(b) The Department of Justice, including the Federal Bureau of Investigation, will reduce domestic terrorist threats, and investigate and prosecute actual or attempted terrorist attacks on, sabotage of, or disruptions of critical infrastructure and key resources. The Attorney General and the Secretary shall use applicable statutory authority and attendant mechanisms for cooperation and coordination, including but not limited to those established by presidential directive.

(c) The Department of Commerce, in coordination with the Department, will work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act to assure the timely availability of industrial products, materials, and services to meet homeland security requirements.

(d) A Critical Infrastructure Protection Policy Coordinating Committee will advise the Homeland Security Council on interagency policy related to physical and cyber infrastructure protection. This PCC will be chaired by a Federal officer or employee designated by the Assistant to the President for Homeland Security.

(e) The Office of Science and Technology Policy, in coordination with the Department, will coordinate interagency research and development to enhance the protection of critical infrastructure and key resources.

(f) The Office of Management and Budget (OMB) shall oversee the implementation of government-wide policies, principles, standards, and guidelines for Federal government computer security programs. The Director of OMB will ensure the operation of a central Federal information security incident center consistent with the requirements of the Federal Information Security Management Act of 2002.

(g) Consistent with the E-Government Act of 2002, the Chief Information Officers Council shall be the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of information resources of Federal departments and agencies.

(h) The Department of Transportation and the Department will collaborate on all matters relating to transportation security and transportation infrastructure protection. The Department of Transportation is responsible for operating the national air space system. The Department of Transportation and the Department will collaborate in regulating the transportation of hazardous materials by all modes (including pipelines).

(i) All Federal departments and agencies shall work with the sectors relevant to their responsibilities to reduce the consequences of catastrophic failures not caused by terrorism.

(23) The heads of all Federal departments and agencies will coordinate and cooperate with the Secretary as appropriate and consistent with their own responsibilities for protecting critical infrastructure and key resources.

(24) All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. Consistent with the Federal Information Security Management Act of 2002, agencies will identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Coordination with the Private Sector

(25) In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms:

(a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and

(b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

National Special Security Events

(26) The Secretary, after consultation with the Homeland Security Council, shall be responsible for designating events as "National Special Security Events" (NSSEs). This directive supersedes language in previous presidential directives regarding the designation of NSSEs that is inconsistent herewith.

Implementation

(27) Consistent with the Homeland Security Act of 2002, the Secretary shall produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives within 1 year from the issuance of this directive. The Plan shall include, in addition to other Homeland Security-related elements as the Secretary deems appropriate, the following elements:

(a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department intends to work with Federal departments and agencies, State and local governments, the private sector, and foreign countries and international organizations;

(b) a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources;

(c) a summary of initiatives for sharing critical infrastructure and key resources information and for providing critical infrastructure and key resources threat warning data to State and local governments and the private sector; and

(d) coordination and integration, as appropriate, with other Federal emergency management and preparedness activities including the National Response Plan and applicable national preparedness goals.

(28) The Secretary, consistent with the Homeland Security Act of 2002 and other applicable legal authorities and presidential guidance, shall establish appropriate systems, mechanisms, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources with other Federal departments and agencies, State and local governments, and the private sector in a timely manner.

(29) The Secretary will continue to work with the Nuclear Regulatory Commission and, as appropriate, the Department of Energy in order to ensure the necessary protection of:

(a) commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training;

(b) nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and

(c) the transportation, storage, and disposal of nuclear materials and waste.

(30) In coordination with the Director of the Office of Science and Technology Policy, the Secretary shall prepare on an annual basis a Federal Research and Development Plan in support of this directive.

(31) The Secretary will collaborate with other appropriate Federal departments and agencies to develop a program, consistent with applicable law, to geospatially map, image, analyze, and sort critical infrastructure and key resources by utilizing commercial satellite and airborne systems, and existing capabilities within other agencies. National technical means should be considered as an option of last resort. The Secretary, with advice from the Director of Central Intelligence, the Secretaries of Defense and the Interior, and the heads of other appropriate Federal departments and agencies, shall develop mechanisms for accomplishing this initiative. The Attorney General shall provide legal advice as necessary.

(32) The Secretary will utilize existing, and develop new, capabilities as needed to model comprehensively the potential implications of terrorist exploitation of vulnerabilities in critical infrastructure and key resources, placing specific focus on densely populated areas. Agencies with relevant modeling capabilities shall cooperate with the Secretary to develop appropriate mechanisms for accomplishing this initiative.

(33) The Secretary will develop a national indications and warnings architecture for infrastructure protection and capabilities that will facilitate:

(a) an understanding of baseline infrastructure operations;

(b) the identification of indicators and precursors to an attack; and

(c) a surge capacity for detecting and analyzing patterns of potential attacks.

In developing a national indications and warnings architecture, the Department will work with Federal, State, local, and non-governmental entities to develop an integrated view of physical and cyber infrastructure and key resources.

(34) By July 2004, the heads of all Federal departments and agencies shall develop and submit to the Director of the OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

(35) On an annual basis, the Sector-Specific Agencies shall report to the Secretary on their efforts to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in their respective sectors. The report shall be submitted within 1 year from the issuance of this directive and on an annual basis thereafter.

(36) The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs will lead a national security and emergency preparedness communications policy review, with the heads of the appropriate Federal departments and agencies, related to convergence and next generation architecture. Within 6 months after the issuance of this directive, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall submit for my consideration any recommended changes to such policy.

(37) This directive supersedes Presidential Decision Directive/NSC-63 of May 22, 1998 ("Critical Infrastructure Protection"), and any Presidential directives issued prior to this directive to the extent of any inconsistency. Moreover, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall jointly submit for my consideration a Presidential directive to make changes in Presidential directives issued prior to this date that conform such directives to this directive.

(38) This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

GEORGE W. BUSH

# # #

Return to this article at:
http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release February 12, 2013

February 12, 2013

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.

Policy

It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.

The Federal Government shall also engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States on which the Nation depends.

U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency. This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors.

Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience:

1) Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure shall be addressed in the plans and execution of the requirements in the National Continuity Policy.

Federal departments and agencies shall implement this directive in a manner consistent with applicable law, Presidential directives, and Federal regulations, including those protecting privacy, civil rights, and civil liberties. In addition, Federal departments and agencies shall protect all information associated with carrying out this directive consistent with applicable legal authorities and policies.

Roles and Responsibilities

Effective implementation of this directive requires a national unity of effort pursuant to strategic guidance from the Secretary of Homeland Security. That national effort must include expertise and day-to-day engagement from the Sector-Specific Agencies (SSAs) as well as the specialized or support capabilities from other Federal departments and agencies, and

strong collaboration with critical infrastructure owners and operators and SLTT entities. Although the roles and responsibilities identified in this directive are directed at Federal departments and agencies, effective partnerships with critical infrastructure owners and operators and SLTT entities are imperative to strengthen the security and resilience of the Nation's critical infrastructure.

Secretary of Homeland Security

The Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. In carrying out the responsibilities assigned in the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure.

Additional roles and responsibilities for the Secretary of Homeland Security include:

1) Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences, in coordination with SSAs and other Federal departments and agencies;
2) Maintain national critical infrastructure centers that shall provide a situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure;
3) In coordination with SSAs and other Federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure;
4) Conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs and in collaboration with SLTT entities and critical infrastructure owners and operators;
5) Coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities;
6) Support the Attorney General and law enforcement agencies with their responsibilities to investigate and prosecute threats to and attacks against critical infrastructure;
7) Coordinate with and utilize the expertise of SSAs and other appropriate Federal departments and agencies to map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies; and

8) Report annually on the status of national critical infrastructure efforts as required by statute.

Sector-Specific Agencies

Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified Sector-Specific Agency that has institutional knowledge and specialized expertise about the sector. Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, SSAs shall carry out the following roles and responsibilities for their respective sectors:

1) As part of the broader national effort to strengthen the security and resilience of critical infrastructure, coordinate with the Department of Homeland Security (DHS) and other relevant Federal departments and agencies and collaborate with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT entities, as appropriate, to implement this directive;
2) Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities;
3) Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;
4) Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and
5) Support the Secretary of Homeland Security's statutorily required reporting requirements by providing on an annual basis sector-specific critical infrastructure information.

Additional Federal Responsibilities

The following departments and agencies have specialized or support functions related to critical infrastructure security and resilience that shall be carried out by, or along with, other Federal departments and agencies and independent regulatory agencies, as appropriate.

1) The Department of State, in coordination with DHS, SSAs, and other Federal departments and agencies, shall engage foreign governments and international organizations to strengthen the security and resilience of critical infrastructure located outside the United States and to facilitate the overall exchange of best practices and lessons learned for promoting the security and resilience of critical infrastructure on which the Nation depends.
2) The Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), shall lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors. DOJ shall investigate, disrupt, prosecute, and otherwise reduce foreign intelligence, terrorist, and other threats to, and actual or attempted attacks on, or sabotage of, the Nation's critical infrastructure. The FBI also conducts domestic collection, analysis, and dissemination of cyber threat information, and shall be responsible for the operation of the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from DHS, the Intelligence Community (IC), the Department of

Defense (DOD), and other agencies as appropriate. The Attorney General and the Secretary of Homeland Security shall collaborate to carry out their respective critical infrastructure missions.

3) The Department of the Interior, in collaboration with the SSA for the Government Facilities Sector, shall identify, prioritize, and coordinate the security and resilience efforts for national monuments and icons and incorporate measures to reduce risk to these critical assets, while also promoting their use and enjoyment.
4) The Department of Commerce (DOC), in collaboration with DHS and other relevant Federal departments and agencies, shall engage private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems, and promote the development of other efforts related to critical infrastructure to enable the timely availability of industrial products, materials, and services to meet homeland security requirements.
5) The IC, led by the Director of National Intelligence (DNI), shall use applicable authorities and coordination mechanisms to provide, as appropriate, intelligence assessments regarding threats to critical infrastructure and coordinate on intelligence and other sensitive or proprietary information related to critical infrastructure. In addition, information security policies, directives, standards, and guidelines for safeguarding national security systems shall be overseen as directed by the President, applicable law, and in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.
6) The General Services Administration, in consultation with DOD, DHS, and other departments and agencies as appropriate, shall provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure.
7) The Nuclear Regulatory Commission (NRC) is to oversee its licensees' protection of commercial nuclear power reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings, and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste. The NRC is to collaborate, to the extent possible, with DHS, DOJ, the Department of Energy, the Environmental Protection Agency, and other Federal departments and agencies, as appropriate, on strengthening critical infrastructure security and resilience.
8) The Federal Communications Commission, to the extent permitted by law, is to exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends.

9) Federal departments and agencies shall provide timely information to the Secretary of Homeland Security and the national critical infrastructure centers necessary to support cross-sector analysis and inform the situational awareness capability for critical infrastructure.

Three Strategic Imperatives

1) Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience

An effective national effort to strengthen critical infrastructure security and resilience must be guided by a national plan that identifies roles and responsibilities and is informed by the expertise, experience, capabilities, and responsibilities of the SSAs, other Federal departments and agencies with critical infrastructure roles, SLTT entities, and critical infrastructure owners and operators.

During the past decade, new programs and initiatives have been established to address specific infrastructure issues, and priorities have shifted and expanded. As a result, Federal functions related to critical infrastructure security and resilience shall be clarified and refined to establish baseline capabilities that will reflect this evolution of knowledge, to define relevant Federal program functions, and to facilitate collaboration and information exchange between and among the Federal Government, critical infrastructure owners and operators, and SLTT entities.

As part of this refined structure, there shall be two national critical infrastructure centers operated by DHS – one for physical infrastructure and another for cyber infrastructure. They shall function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure. Just as the physical and cyber elements of critical infrastructure are inextricably linked, so are the vulnerabilities. Accordingly, an integration and analysis function (further developed in Strategic Imperative 3) shall be implemented between these two national centers.

The success of these national centers, including the integration and analysis function, is dependent on the quality and timeliness of the information and intelligence they receive from the SSAs and other Federal departments and agencies, as well as from critical infrastructure owners and operators and SLTT entities.

These national centers shall not impede the ability of the heads of Federal departments and agencies to carry out or perform their responsibilities for national defense, criminal, counterintelligence, counterterrorism, or investigative activities.

2) Enable Efficient Information Exchange by Identifying Baseline Data and Systems Requirements for the Federal Government

A secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical

infrastructure owners and operators. This must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents. The goal is to enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems.

Greater information sharing within the government and with the private sector can and must be done while respecting privacy and civil liberties. Federal departments and agencies shall ensure that all existing privacy principles, policies, and procedures are implemented consistent with applicable law and policy and shall include senior agency officials for privacy in their efforts to govern and oversee information sharing properly.

3) Implement an Integration and Analysis Function to Inform Planning and Operational Decisions Regarding Critical Infrastructure

The third strategic imperative builds on the first two and calls for the implementation of an integration and analysis function for critical infrastructure that includes operational and strategic analysis on incidents, threats, and emerging risks. It shall reside at the intersection of the two national centers as identified in Strategic Imperative 1, and it shall include the capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information to:

a. Aid in prioritizing assets and managing risks to critical infrastructure;
b. Anticipate interdependencies and cascading impacts;
c. Recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident; and
d. Support incident management and restoration efforts related to critical infrastructure.

This function shall not replicate the analysis function of the IC or the National Counterterrorism Center, nor shall it involve intelligence collection activities. The IC, DOD, DOJ, DHS, and other Federal departments and agencies with relevant intelligence or information shall, however, inform this integration and analysis capability regarding the Nation's critical infrastructure by providing relevant, timely, and appropriate information to the national centers. This function shall also use information and intelligence provided by other critical infrastructure partners, including SLTT and nongovernmental analytic entities.

Finally, this integration and analysis function shall support DHS's ability to maintain and share, as a common Federal service, a near real-time situational awareness capability for critical infrastructure that includes actionable information about imminent threats, significant trends, and awareness of incidents that may affect critical infrastructure.

Innovation and Research and Development

The Secretary of Homeland Security, in coordination with the Office of Science and Technology Policy (OSTP), the SSAs, DOC, and other Federal departments and agencies, shall provide input to align those Federal and Federally-funded research and development (R&D) activities that seek to strengthen the security and resilience of the Nation's critical infrastructure, including:

1) Promoting R&D to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;
2) Enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario, as well as cascading effects on other sectors;
3) Facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen all-hazards security and resilience; and
4) Prioritizing efforts to support the strategic guidance issued by the Secretary of Homeland Security.

Implementation of the Directive

The Secretary of Homeland Security shall take the following actions as part of the implementation of this directive.

1) Critical Infrastructure Security and Resilience Functional Relationships. Within 120 days of the date of this directive, the Secretary of Homeland Security shall develop a description of the functional relationships within DHS and across the Federal Government related to critical infrastructure security and resilience. It should include the roles and functions of the two national critical infrastructure centers and a discussion of the analysis and integration function. When complete, it should serve as a roadmap for critical infrastructure owners and operators and SLTT entities to navigate the Federal Government's functions and primary points of contact assigned to those functions for critical infrastructure security and resilience against both physical and cyber threats. The Secretary shall coordinate this effort with the SSAs and other relevant Federal departments and agencies. The Secretary shall provide the description to the President through the Assistant to the President for Homeland Security and Counterterrorism.

2) Evaluation of the Existing Public-Private Partnership Model. Within 150 days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators, shall conduct an analysis of the existing public-private partnership model and recommend options for improving the effectiveness of the partnership in both the physical and cyber space. The evaluation shall consider options to streamline processes for collaboration and exchange of information and to minimize duplication of effort. Furthermore, the analysis shall consider how the model can be flexible and adaptable to meet the unique needs of individual sectors while providing a focused, disciplined, and effective approach for the Federal Government to coordinate with the critical infrastructure owners and operators and with SLTT governments. The evaluation shall result in recommendations to enhance partnerships to be approved for implementation through the

processes established in the Organization of the National Security Council System directive.

3) Identification of Baseline Data and Systems Requirements for the Federal Government to Enable Efficient Information Exchange. Within 180 days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs and other Federal departments and agencies, shall convene a team of experts to identify baseline data and systems requirements to enable the efficient exchange of information and intelligence relevant to strengthening the security and resilience of critical infrastructure. The experts should include representatives from those entities that routinely possess information important to critical infrastructure security and resilience; those that determine and manage information technology systems used to exchange information; and those responsible for the security of information being exchanged. Interoperability with critical infrastructure partners; identification of key data and the information requirements of key Federal, SLTT, and private sector entities; availability, accessibility, and formats of data; the ability to exchange various classifications of information; and the security of those systems to be used; and appropriate protections for individual privacy and civil liberties should be included in the analysis. The analysis should result in baseline requirements for sharing of data and interoperability of systems to enable the timely exchange of data and information to secure critical infrastructure and make it more resilient. The Secretary shall provide that analysis to the President through the Assistant to the President for Homeland Security and Counterterrorism.

4) Development of a Situational Awareness Capability for Critical Infrastructure. Within 240 days of the date of this directive, the Secretary of Homeland Security shall demonstrate a near real-time situational awareness capability for critical infrastructure that includes threat streams and all-hazards information as well as vulnerabilities; provides the status of critical infrastructure and potential cascading effects; supports decision making; and disseminates critical information that may be needed to save or sustain lives, mitigate damage, or reduce further degradation of a critical infrastructure capability throughout an incident. This capability should be available for and cover physical and cyber elements of critical infrastructure, and enable an integration of information as necessitated by the incident.

5) Update to National Infrastructure Protection Plan. Within 240 days of the date of this directive, the Secretary of Homeland Security shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a successor to the National Infrastructure Protection Plan to address the implementation of this directive, the requirements of Title II of the Homeland Security Act of 2002 as amended, and alignment with the National Preparedness Goal and System required by PPD-8. The plan shall include the identification of a risk management framework to be used to strengthen the security and resilience of critical infrastructure; the methods to be used to prioritize critical infrastructure; the protocols to be used to synchronize communication and actions within the Federal Government; and a metrics and analysis process to be used to measure the Nation's ability to manage and reduce risks to

critical infrastructure. The updated plan shall also reflect the identified functional relationships within DHS and across the Federal Government and the updates to the public-private partnership model. Finally, the plan should consider sector dependencies on energy and communications systems, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems. The Secretary shall coordinate this effort with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators.

6) National Critical Infrastructure Security and Resilience R&D Plan. Within 2 years of the date of this directive, the Secretary of Homeland Security, in coordination with the OSTP, the SSAs, DOC, and other Federal departments and agencies, shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a National Critical Infrastructure Security and Resilience R&D Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments. The plan should be issued every 4 years after its initial delivery, with interim updates as needed.

Policy coordination, dispute resolution, and periodic in-progress reviews for the implementation of this directive shall be carried out consistent with PPD-1, including the use of Interagency Policy Committees coordinated by the National Security Staff.

Nothing in this directive alters, supersedes, or impedes the authorities of Federal departments and agencies, including independent regulatory agencies, to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives, including, but not limited to, the designation of critical infrastructure under such authorities.

This directive revokes Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, issued December 17, 2003. Plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

Designated Critical Infrastructure Sectors and Sector-Specific Agencies

This directive identifies 16 critical infrastructure sectors and designates associated Federal SSAs. In some cases co-SSAs are designated where those departments share the roles and responsibilities of the SSA. The Secretary of Homeland Security shall periodically evaluate the need for and approve changes to critical infrastructure sectors and shall consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated SSA for that sector. The sectors and SSAs are as follows:

Chemical:
Sector-Specific Agency: Department of Homeland Security

Commercial Facilities:
Sector-Specific Agency: Department of Homeland Security

Communications:
Sector-Specific Agency: Department of Homeland Security

Critical Manufacturing:
Sector-Specific Agency: Department of Homeland Security

Dams:
Sector-Specific Agency: Department of Homeland Security

Defense Industrial Base:
Sector-Specific Agency: Department of Defense

Emergency Services:
Sector-Specific Agency: Department of Homeland Security

Energy:
Sector-Specific Agency: Department of Energy

Financial Services:
Sector-Specific Agency: Department of the Treasury

Food and Agriculture:
Co-Sector-Specific Agencies: U.S. Department of Agriculture and Department of Health and Human Services

Government Facilities:
Co-Sector-Specific Agencies: Department of Homeland Security and General Services Administration

Healthcare and Public Health:
Sector-Specific Agency: Department of Health and Human Services

Information Technology:
Sector-Specific Agency: Department of Homeland Security

Nuclear Reactors, Materials, and Waste:
Sector-Specific Agency: Department of Homeland Security

Transportation Systems:
Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation

Water and Wastewater Systems:
Sector-Specific Agency: Environmental Protection Agency

Definitions

For purposes of this directive:

The term "all hazards" means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

The term "collaboration" means the process of working together to achieve shared goals.

The terms "coordinate" and "in coordination with" mean a consensus decision-making process in which the named coordinating department or agency is responsible for working with the affected departments and agencies to achieve consensus and a consistent course of action.

The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

The term "Federal departments and agencies" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

The term "national essential functions" means that subset of Government functions that are necessary to lead and sustain the Nation during a catastrophic emergency.

The term "primary mission essential functions" means those Government functions that must be performed in order to support or implement the performance of the national essential functions before, during, and in the aftermath of an emergency.

The term "national security systems" has the meaning given to it in the Federal Information Security Management Act of 2002 (44 U.S.C. 3542(b)).

The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

The term "Sector-Specific Agency" (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

The terms "secure" and "security" refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

# # #

Dams Sector
Government Coordinating Council
Charter

1. Official Designation

The official designation of this Council is the "Dams Sector Government Coordinating Council," hereinafter referred to as the "GCC" or the "Council."

2. Governance

GCC members will make decisions through a consultative process, encourage the exchange of information and points of view, and strive for consensus. Although any member may disagree with a decision, other members will strive to understand and close the gaps creating the disagreement. Dissension will be recognized and reasons clearly understood by all other members when a member absolutely cannot agree. When there is dissension, the GCC may move forward and take action, nevertheless, to fulfill the obligations of the Council. GCC members will strive to meet timelines and deliverables even when there is less than full agreement.

The GCC recognizes that each member is a government entity or organization with inherent legal authorities and parameters within which they must operate. At times, these authorities may restrict a member's ability to provide agreement on a decision or preclude the dissemination of information to certain members due to classification restrictions and/or inadequate security clearances of member representatives. These inherent legal authorities must be clearly articulated and understood by the GCC when they are the basis for dissent and the inability to enter into consensus.

Council members shall strive to faithfully represent the position of their individual government agencies; however, the GCC recognizes that representatives may lack legal authority to act on behalf of their agencies. Therefore, the actions of the GCC or of individual members may not be binding on a government agency.

3. Objective

The objective of the GCC is to provide effective coordination and communication of Dams Sector security and security-related strategies, safety activities, and policy across and between government agencies, and between the agencies and the sector to support the Nation's homeland security mission. The GCC shall support the implementation of Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, and shall act as the counterpart and partner to the private, industry-led Dams Sector Coordinating Council (SCC) to plan, implement and execute sector-wide security programs for the Nation's dams, locks, levees and other infrastructure assets within the Dams Sector.

The GCC serves as an effective mechanism to increase the amount of coordination and information sharing among member agencies; improve integration of safety and security initiatives; enhance effective dialog among owners, regulators, non-government owners, and other sector security partners; foster coordination with other critical infrastructure/key resource (CIKR) sectors; and promote implementation of regional disaster resilience initiatives.

4. Scope of Activity

The GCC will accomplish this objective through the following essential activities:

- Identifying sector issues that require public-private coordination and communication. The GCC shall bring together diverse government interests to identify and develop collaborative national strategies that advance the safety, security and protection of CIKR. The GCC shall support the policies, processes/protocols and technology that enable the sharing of this information among government and private sector entities, as well as international partners.

- Identifying and assessing sector interdependencies, vulnerabilities, and opportunities for increasing the sector's resiliency. The GCC shall help build national awareness on issues related to preparedness, recovery and reconstitution of Dams Sector infrastructure affected by large-scale disasters caused by a terrorist attack, natural disaster, or other incidents.

- Identifying and promoting successful programs and practices which contribute to the development of a sustainable and resilient national infrastructure. The GCC shall facilitate the sharing of experiences, ideas, lessons learned and innovative approaches related to the safety, security, and protection of critical infrastructure.

- Identifying complementary security efforts and leveraging resources within government and between government and other stakeholders that can be utilized to further the development of consistent, sustainable, effective and measurable plans for sector-wide security programs.

5. Membership

5.1 Permanent Members

GCC permanent membership is composed of government agencies that own, operate or regulate sector assets or have responsibility for security and protection of those assets. Permanent membership resides with the agency rather than the agency representatives. GCC permanent membership includes voting and non-voting agency members. Each member agency shall have a primary and an alternate representative to the GCC. Primary agency representatives named to the GCC are director/manager-level, or equivalent.

Voting Members:

- U.S. Department of Agriculture, Natural Resources Conservation Service
- U.S. Department of Defense, U.S. Army Corps of Engineers
- U.S. Department of Homeland Security, Office of Infrastructure Protection
- U.S. Department of the Interior, Bureau of Reclamation
- U.S. Department of Labor, Mine Safety and Health Administration
- U.S. Department of State, International Boundary and Water Commission
- Federal Energy Regulatory Commission

- Tennessee Valley Authority
- Eight (8) State Dam Safety Offices

Non-Voting Members:

- Bonneville Power Administration
- Environmental Protection Agency
- Federal Emergency Management Agency
- National Weather Service
- U.S. Coast Guard
- U.S. Department of Energy

5.2 Ad-Hoc Members

The GCC may also include individuals that serve as designated liaisons from other Department of Homeland Security components and directorates, other sector and cross-sector GCCs, other government agencies, and international governmental entities that are invited to participate in GCC meetings and activities as ad-hoc, non-voting members to provide relevant institutional knowledge and technical expertise.

6. Roles and Responsibilities

GCC leadership rests with the primary and alternate representatives from the DHS/IP/Sector Specific Agency Executive Management Office (SSA EMO). The SSA EMO is the designated Sector Specific Agency representative on behalf of DHS/IP. The GCC Chairman is the Director of the SSA EMO and will designate an alternate to assist him/her and/or act on his/her behalf as necessary. The GCC leadership will collect issues from other members and initiate or bring issues to the Council for consideration and deliberation. The GCC leadership will monitor and assure that initiatives or issues are brought to closure.

There are 16 voting members of the GCC; one voting representative for each of the eight Federal agencies and the eight member States. An alternate member representative casts the member's vote in the absence of the primary representative.

All members of the GCC are responsible for obtaining and maintaining, for their representatives, the appropriate security clearances required for discussing and sharing sensitive but unclassified and classified information. This information will be protected and handled in accordance with the originating agency's guidelines and requirements for information security. DHS will manage the security clearance process for representatives from member States.

The GCC Secretariat, provided by DHS/IP/Partnership and Outreach Division, will support all GCC activities.

7. Workgroups

Workgroups are established when substantial investigation, research or other tasks are required which cannot be practicably achieved at regular GCC sessions. All products of the workgroups are meant to advise Council members on various issues and processes. Through their primary or alternate representatives, each member agency may designate individuals to serve on workgroups or act as workgroup leads.

The GCC establishes workgroups that:

- Consist of personnel selected by the GCC based on the issue under study and its scope;
- Have a specific and clearly defined mission and scope, time limit, and deliverable(s);
- Select a workgroup lead charged with ensuring that the workgroup achieves its mission and stays within scope; and
- Receive support from the Secretariat as needed.

When the GCC and SCC form joint workgroups, the GCC workgroup lead will work in close coordination with the corresponding SCC workgroup lead.

8. Number and Frequency of Meetings

The GCC will meet quarterly in Washington, DC and/or in an alternative destination if decided by a majority of the Council members, with additionally scheduled meetings and/or conference calls as needed.

9. Modification of Charter

The charter may be modified by affirmative vote, which must consist of the quorum plus one, of the voting members.

Dams Sector
Government Coordinating Council
Charter

List of Dams GCC Signatories as of November 2008

Noller Herbert
U.S. Department of Agriculture, Natural Resources Conservation Service

David Gutierrez
State Dam Safety Office of California

Edward Hecker
U.S. Department of Defense, U.S. Army Corps of Engineers

Mark Haynes
State Dam Safety Office of Colorado

W. Craig Conklin
U.S. Department of Homeland Security, Office of Infrastructure Protection

Patrick Diederich
State Dam Safety Office of Nebraska

David G. Achterberg
U.S. Department of the Interior, Bureau of Reclamation

John Moyle
State Dam Safety Office of New Jersey

John Fredland
U.S. Department of Labor, Mine Safety and Health Administration

Steve McEvoy
State Dam Safety Office of North Carolina

Al Riera
U.S. Department of State, International Boundary and Water Commission

Keith Banachowski
State Dam Safety Office of Ohio

Daniel Mahoney
Federal Energy Regulatory Commission

Dennis Dickey
State Dam Safety Office of Pennsylvania

Robert T. Parker
Tennessee Valley Authority

Douglas Johnson
State Dam Safety Office of Washington

ANNEX A

Standard Operating Procedures

Quorum

A quorum for decision-making is defined as consisting of primary representatives from four Federal agency GCC members and four State agency GCC members, or their designated alternates.

Process

Council meeting procedures will follow Robert's Rules of Order. GCC members will make decisions through a consultative process, encouraging the exchange of information and points of view, and will strive for consensus.

Principles of Participation

- All members must be working towards the same goal and purpose of improving the safety, security, preparedness, resilience, recovery and reconstitution of Dams Sector assets.
- All members need to participate in order to achieve the Council's objective.
- Discussion and deliberation processes must recognize and take advantage of each member's strengths, skills, and perspective.
- Results of GCC discussions and deliberations must constitute a coherent voice made up of each member's contributions.
- Discussions shall be honest and forthright.

Meeting Support

The GCC Secretariat will:

- Consult with GCC leadership to provide support for developing agendas, and maintaining a calendar for GCC and joint GCC/SCC council meetings;
- Provide to all members, no later than one week before the meeting, a set of read-ahead materials, including the agenda and any other preparatory documents;
- Compile the minutes of each meeting and provide to GCC members, with the leader's concurrence, within two weeks of the meeting for review and concurrence by all members;
- Assist in the development of the logistics for GCC meetings, whether in person or teleconference; and
- Provide additional support to workgroups as needed.

Day to Day Communications

The Secretariat will assist in maintaining and updating the contact list of GCC representatives that will be used for GCC communications.

Observers

GCC members may invite observers to attend GCC meetings. Members extending an invitation are to notify the GCC Secretariat of the invitation in advance of the meeting.

Closed Session

The GCC may elect, by majority vote, to close the meeting to all but permanent members.

ANNEX B

State Dam Safety Offices

The following is a list of primary representatives from State Dam Safety Offices that are currently voting members of the Dams Sector Government Coordinating Council:

California: David Gutierrez

Colorado: Mark Haynes

Nebraska: Patrick Diederich

New Jersey: John Moyle

North Carolina: Steve McEvoy

Ohio: Keith Banachowski

Pennsylvania: Dennis Dickey

Washington: Douglas Johnson