~~SECRET//NOFORN~~

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHREN DISTRIT OF CALIFORNIA (OAKLAND)

CAITLIN KELLY HENRY AND JESSE ABRAM STOUT, Plaintiffs, v. FEDERAL BUREAU OF INVESTIGATION, Defendant.	Civil Action No. 4:13-cv-05924-DMR

~~CLASSIFIED~~ Unclassified

THIRD DECLARATION OF DAVID M. HARDY

I, David M. Hardy, declare as follows:

(1) (U) I am the Section Chief of the Record/Information Dissemination Section ("RIDS"), Records Management Division ("RMD"), in Winchester, Virginia. I have held this position since August 1, 2002. Prior to my joining the Federal Bureau of Investigation ("FBI"), from May 1, 2001 to July 31, 2002, I was the Assistant Judge Advocate General of the Navy for Civil Law. In that capacity, I had direct oversight of Freedom of Information Act ("FOIA") policy, procedures, appeals, and litigation for the Navy. From October 1, 1980 to April 30, 2001, I served as a Navy Judge Advocate at various commands and routinely worked with FOIA matters. I am also an attorney who has been licensed to practice law in the State of Texas since 1980.

(2) (U) In my official capacity as Section Chief of RIDS, I supervise approximately 227 employees who staff a total of ten (10) Federal Bureau of Investigation Headquarters ("FBIHQ") units and two (2) field operational service center units whose collective mission is to effectively plan, develop, direct, and manage responses to requests for access to FBI records and

Date: April 13, 2015
Classified By: J37J85T94
Derived From: NSICG
Reason: 1.4_C
Declassify on: April 13, 2040

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

information pursuant to the FOIA as amended by the OPEN Government Act of 2007 and the OPEN FOIA Act of 2009; the Privacy Act of 1974; Executive Order 13526; Presidential, Attorney General, and FBI policies and procedures; judicial decisions; and Presidential and Congressional directives. I have been designated by the Attorney General of the United States as an original classification authority and a declassification authority pursuant to E.O. 13526, §§ 1.3 and 3.1. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

(3) (U) Due to the nature of my official duties, I am familiar with the procedures followed by the FBI in responding to request for information from its files pursuant to the provisions of the FOIA, 5 U.S.C. § 552. Specifically, I am aware of the FBI's handling of all three Freedom of Information/Privacy Act ("FOIPA") requests concerning the plaintiffs.

(4) (U) The FBI submits this declaration in response to the hearing held on February 26, 2015 and Judge Ryu's request for the FBI to submit a supplemental declaration regarding the Data Integration and Visualization System ("DIVS") and the burden associated with searching this database in response to a FOIA request. This declaration incorporates my two previous declarations dated September 25, 2014 ("First Hardy Declaration") and December 8, 2014 ("Second Hardy Declaration"). Moreover, the FBI submits this declaration in further support of the FBI's Motion for Summary Judgment.

THE FBI – AN INTELLIGENCE-GATHERING AGENCY

(5) (U) The FBI began as a domestic agency investigating violations of federal criminal statutes; however, its role significantly changed after the 9/11 terrorist attacks. In response, the FBI's priorities dramatically shifted away from its traditional law enforcement

mission and took on a more expansive role as an intelligence-gathering agency. The FBI now serves a dual function as the country's main internal intelligence agency and federal law enforcement organization. It is the primary and lead domestic security agency investigating U.S. counterterrorism, counterintelligence, and criminal investigative organizations. *See* 28 U.S.C. Chapter 33. The FBI's mission "is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, states, municipal, and international agencies and partners." *See* FBI Mission Statement at http://www.fbi.gov/about-us/quick-facts. Today, the FBI's top three priorities are to protect the United States from terrorist attacks, as well as against foreign intelligence operations and espionage, and cyber-based attacks and high-technology crimes. *Id.*

(6) (U) In the wake of 9/11, the federal government realized its failure to prevent the attacks hinged on federal agencies' inability to share vital intelligence information across agency lines. This desperate need to close the gap between federal agencies, and state and local law enforcement was recognized and highlighted in the passage of the USA PATRIOT Act of 2001[1] and the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRPTA"). The USA PATRIOT Act removed major legal barriers that in the past "prevented law enforcement, intelligence, and national defense communities from talking and coordinating their work to protect the American people and our national security." *See* the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). The Act recognized the need to remove institutional restrictions, and to connect the agencies and their information in a meaningful and effective way.

[1] (U) The "USA PATRTIOT Act" is an acronym for the Uniting and Strengthening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). It is commonly referred to as "the Patriot Act."

"The Patriot Act facilitated information sharing and cooperation among government agencies so that they can better 'connect the dots.'" *Id.* Similarly, the IRPTA recognized the critical need for federal agencies to share information in order to prevent future terrorist attacks. In Chapter IV of the FBI's 9/11 Review Commission Report issued March of 2015, it states under the heading "Collaboration and Information Sharing" that the

> [t]wo fundamental tenets are at the heart of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA): 1) that state and local authorities and the American public are now important partners in maintaining the necessary vigilance, and 2) the FBI and the United States Intelligence Community (USIC) need to work in close partnership to prevent terrorist acts against the Homeland. Together, these beliefs have transformed the environment in which the FBI operates and have changed how success in that environment is defined.

(7) (U) Threats to our national security have multiplied, and become more dangerous and complex. "In the coming decade, these evolving threats will increasingly challenge the FBI's leadership at every level, its traditional culture, and all of its core capabilities in criminal investigation, counterintelligence, intelligence collection and analysis and technology." *See* the 9/11 Review Commission, "The FBI: Protecting the Homeland in the 21st Century," page 17 (March 2015). The Report also states that "[t]he extensive reforms of the past decade must be accelerated to fulfill the Bureau's expanded global mission as a fully integrated, intelligence-driven investigative organization." *Id.* The FBI has accepted its role as America's premier domestic intelligence agency and has taken steps to advance technologically in order to meet our country's ever-changing and increasing security demands.

DIVS – AN INTELLIGENCE-GATHERING TOOL

(8) (S//NF) [redacted]

[redacted]

[2] (U) The authority for the maintenance of this system can be found in the following: 28 U.S.C. Chapter 33; 18 U.S.C. 2332(b); 28 CFR 0.85; the USA PATRIOT Act of 2001; the IRTPA of 2004; the Implementing Recommendations of the 9/11Commission Act of 2007; 42 U.S.C. 3771; the National Security Act of 1947, as amended; Section 603 of the Intelligence Authorization Act of 1990, the Attorney General's Guidelines for Domestic FBI Operations and numerous other statutes, executive orders, and presidential directives.

[3] (S/NF) [redacted]

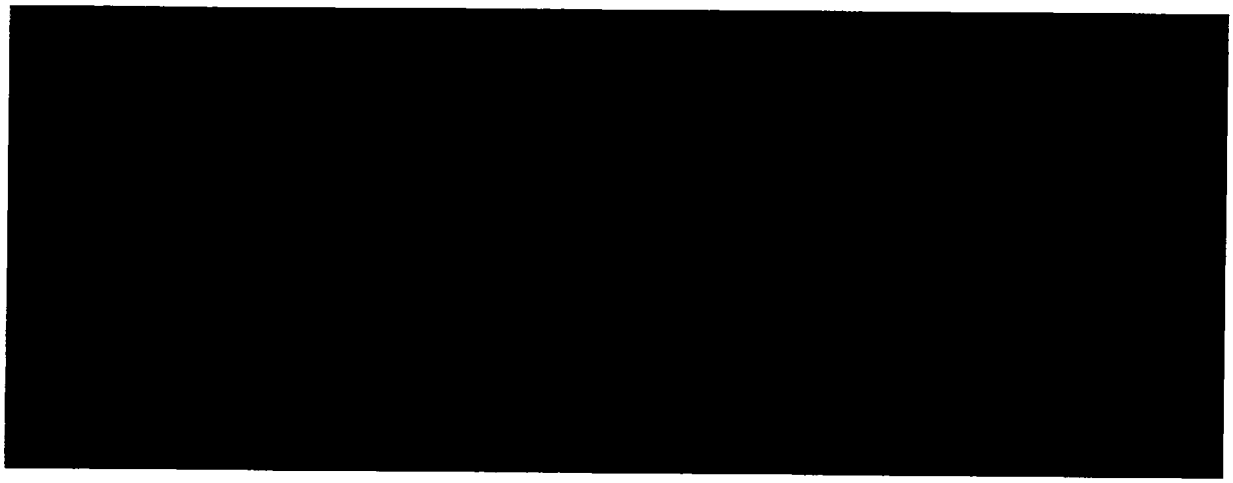
[redacted]

(9) (S//NF) [redacted]

I. **A SEARCH OF DIVS IS UNREASONABLY BURDENSOME**

(10) (U) The FOIA requires agencies to search those locations reasonably calculated to locate responsive records and does not require an agency to conduct "unreasonably burdensome" searches. A search of DIVS is "unreasonably burdensome" in four respects: (i) its use as a FOIA search mechanism is incompatible with its function and design; (ii) it expands FBI's search obligations beyond those required under FOIA, (iii) the search would generate a large number of false positives, (iv) and its FOIA poses an unreasonable administrative hardship.

(11) (S//NF) [redacted]



(12) (U) A search of the DIVS database is "unreasonably burdensome" because its use as a FOIA search mechanism is incompatible with its function and design. Because of its comprehensive nature and scope, the CRS is the primary system used by the FBI to locate information in response to FOIA requests as pertinent information about individuals, organizations, or events are indexed therein for future retrieval via ACS or Sentinel. In contrast, DIVS is a database system with a function and purpose materially different than the CRS. DIVS was created with the purpose of establishing a centralized data warehouse for the compilation, fusion, storage, and comprehensive analysis of pertinent information across multiple agencies. It is designed to function as a search engine/analytical tool to assist Special Agents and Intelligence Analysts with "connecting the dots" by retrieving and filtering information from various agencies and their databases in furtherance of investigative, national security, and intelligence purposes. In contrast, the CRS is the FBI's cornerstone record-keeping system with a universal index designed for rapid and efficient location and retrieval of FBI records. As such, the CRS index searches via the ACS and/or Sentinel case management systems comport with the FBI's

[4] (U) Un-minimized FISA refers to foreign intelligence information collected through electronic surveillance which has not undergone minimization procedures. Minimization procedures refers to a process adopted by the Attorney General which limits the acquisition, retention, and dissemination of non-publicly available information collected concerning un-consenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate intelligence information.

mandate to conduct a reasonable search for records in response to FOIA/PA requests. Simply put, DIVS is an investigative and intelligence tool that harnesses data from multiple agencies and sources; its function and design is incompatible with an FBI FOIA records search.

(13) (U) Second, a search of the DIVS database is "unreasonably burdensome" because it expands the scope of the FBI's FOIA search obligations. The FOIA provides public access to "agency records" that are not exempt and requires agencies to conduct reasonable searches for its records. Here, the FBI conducted index searches of the CRS using ACS (UNI) and Sentinel, both yielding "no records." A DIVS search inherently extends the reach of the FBI's obligation to conduct a reasonable search for its own records because DIVS pulls from multi-agency data sources. Under such a construct, the FBI would carry the unprecedented burden of conducting multi-agency searches, thus triggering the enormous task of retrieving and reviewing each potentially responsive piece of data pulled from DIVS that originated from other government agencies. This unduly expands the scope the FBI's FOIA obligation to locate information in its files.

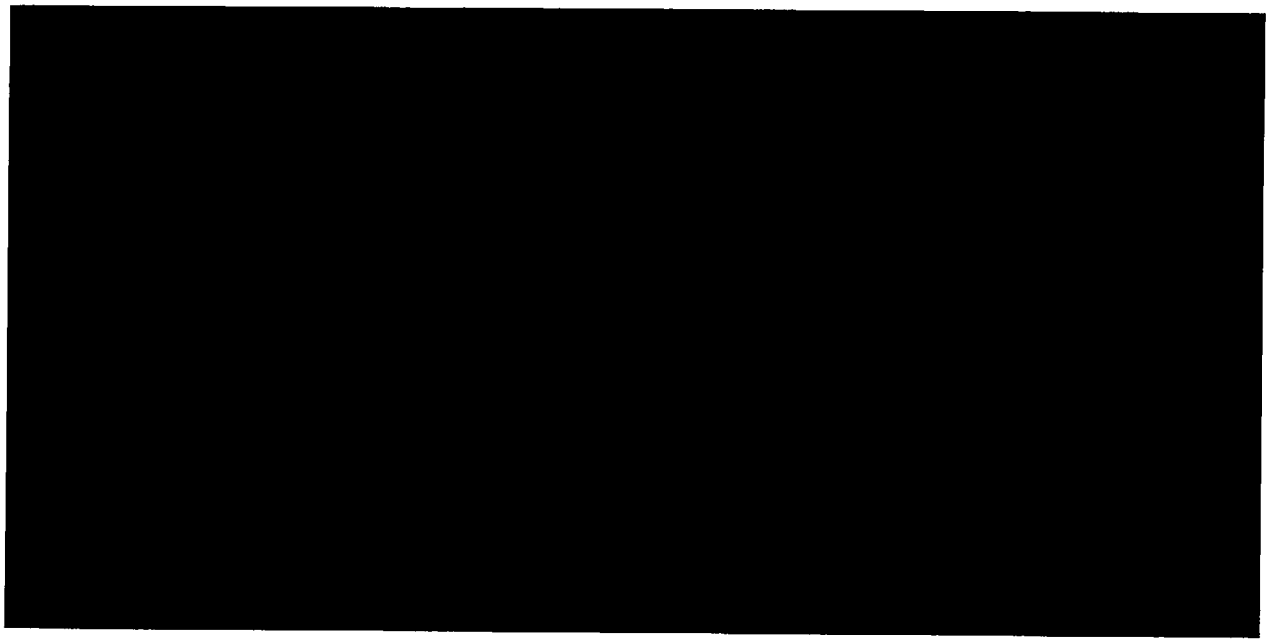
(14) (U) Third, a DIVS search is unreasonably burdensome because it would result in numerous false positives. A DIVS search functions similarly to an ECF text search though its purpose as an analytical tool is inherently different from the recording-keeping purposes of the CRS. The CRS, unlike the DIVS, has a record-keeping function and is set up in a manner that lends itself to indexing records for future retrieval. As explained in the Second Hardy Declaration, an ECF text search allows users to look for specific names or keywords by electronically scanning the text of most FBI documents. This type of search returns a significant number of "hits." These "hits" are generally random and incomplete references, such as mere mentions of a name, absent identifying information in which to confirm the identity of the

individual mentioned. *See* Second Hardy Declaration at ¶¶10-11. The names resulting from a full-text search are usually incomplete or unaccompanied by any identifying information such as a date of birth, social security number, address, phone number, and etc. In most instances, the text reference only consists of a first or last name. An ECF text search returns numerous results requiring RIDS to undergo the arduous task of examining each random "hit" to determine whether the mere mention of an individual is identical to the subject of the search. These additional administrative steps require a significant amount of time and resources, and generally prove fruitless. If RIDS is unable to identify the referenced individual, then the "hit" is a false positive and deemed non-responsive. Similarly, in DIVS, the entirety of every product, within all 122 datasets, is text searchable and would trigger the same false positive concerns posed by an ECF text search. In fact, an ECF text search would be included in any DIVS search because it is one of DIVS' datasets. Compounding the problem is the multi-agency scope of DIVS; a DIVS search is tantamount to an ECF text search of multiple government agencies, thus a name search would result in an even larger number of false positives. The use of finite RIDS resources to sift through scores of false positives originating from across the government does not comport with the principle of conducting a reasonable search in response to a FOIA/PA request.

(15) (U) To highlight the gravity of this incredible undue burden, if the FBI were to begin conducting a DIVS search of individuals in response to FOIA/PA requests, the time and resources expended to respond to such requests would be astronomical. Searching DIVS for common names--"John Smith" for example--would generate an insurmountable number of "hits" to sift through for one request. Simply put, using DIVS as a FOIA tool to locate information about individuals would open the flood gates and constitute an administrative hardship for the FBI by directly impacting its finite resources and affecting its ability to timely respond to other

FOIA requests.

(16) (S//NF) [redacted]



(17) (U) In summary, the use of DIVS to search for information in response to a FOIA/PA request task is inherently unreasonable, unduly burdensome, and would not be reasonably calculated to locate information in response to a request. This search task would simply require so much time per request that it would effectively shut down the FBI's ability to respond to the thousands of requests it receives annually from citizens for information in FBI records. Currently, the FBI has a total of 5,070 pending FOIA requests for FY 2015. In other words, using DIVS as a FOIA search mechanism poses a burden so large and unreasonable to RIDS that it equates to a denial of service to other requesters.

II. DIVS CONTENTS ARE OTHERWISE EXEMPT FROM DISCLOSURE UNDER FOIA EXEMPTIONS (b)(1), (b)(3), and (b)(7)(E)

(18) (U) Burdensomeness aside, a DIVS search would not produce information that can be released; public dissemination is prohibited either through executive order, statute, or pursuant to a FOIA Exemption. With the exception of information that would be duplicative to information located through a CRS search, the DIVS database and its content would be exempt from disclosure pursuant to FOIA Exemptions (b)(1), (b)(3), and (b)(7)(E).

A. Exemption (b)(1) - Classified Information
E.O. 13526, § 1.4(c) - Intelligence Activities, Sources, and Methods

(19) (U) FOIA Exemption (b)(1) prohibits from disclosure information that is specifically authorized "under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy" and "is in fact properly classified pursuant to such Executive Order." *See* 5 U.S.C. § 552 (b)(1). Executive Order 13526, signed by President Barack Obama on December 29, 2009, is the current order which allows for the protection of national security information. "National Security" is defined as "the national defense of foreign relations of the United States." *See* Section 1.6 (cc) of E.O. 13526.

(20) (U) Certain substantive requirements must be met before information can be deemed classified. Those requirements include: (1) an original classification authority is classifying the information; (2) the information is owned by; produced by or for, or is under the control of the United States Government; (3) the information falls within one or more of the categories of information listed in § 1.4 of this order[5]; and (4) the original classification authority determines the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage. *See* E.O. 13526, § 1.1 (a). Although there are no DIVS accessed records to examine in the instant case, as an

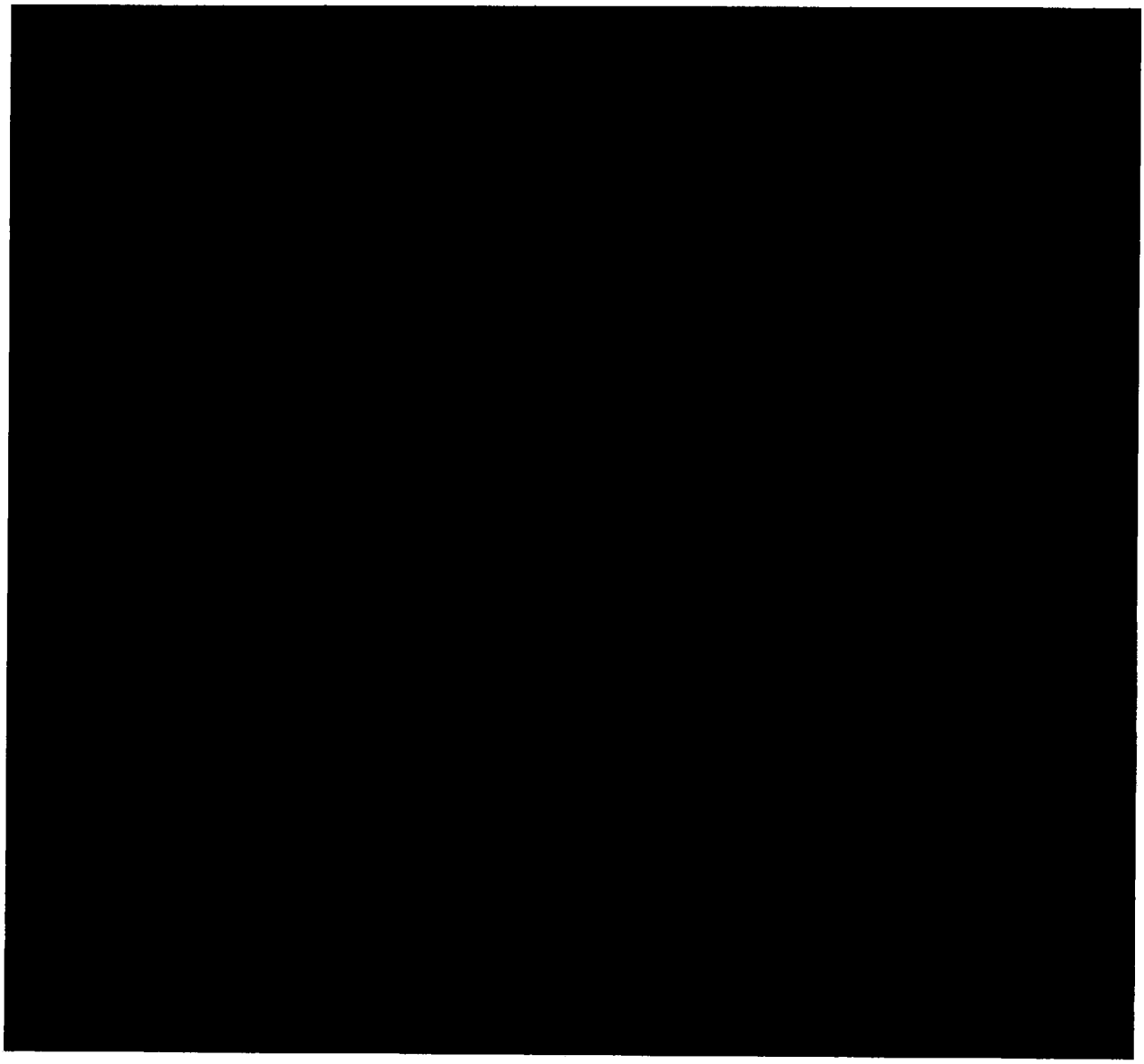
[5] (U) Under E.O. 13526, § 1.4, information shall be considered classified if the unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to national security; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or (h) the development, production, or use of weapons of mass destruction.

original classification authority, I can conclude DIVS content would readily qualify for classification and withholding under Exemption (b)(1) because DIVS is itself an intelligence source and method. *See* Operational Declaration at ¶¶ 10-11. DIVS content would readily meet the four (4) substantive requirements as the datasets are owned by and under the control of the United States Government; the use of DIVS and its resulting product would reveal information under § 1.4(c), intelligence activities as well as intelligence sources and methods; and such unauthorized disclosure reasonably could be expected to cause serious or exceptionally grave damage to the national security.[6]

(21) (U) More specifically, E.O. 13526, § 1.4(c), exempts from disclosure intelligence activities (including covert action), intelligence sources or methods, or cryptology. An intelligence activity or method includes any intelligence action or technique utilized by the FBI against a targeted individual or organization who has been determined to be of national security interest. An intelligence method is used to indicate any procedure (human or non-human) utilized to obtain information concerning such individual or organization. An intelligence activity or method has two characteristics. First, the intelligence activity or method -- and information generated by it -- is needed by U. S. Intelligence Community to carry out its foreign intelligence and counterintelligence missions. Second, confidentiality must be maintained with respect to the activity or method if the viability, productivity and usefulness of this information is to be preserved.

(22) (S//NF) [redacted]

[6] (U) Classification markings at the "Secret" level requires that "the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security." "Top Secret" markings are warranted when "the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security." See E.O. 13526 § 1.2(a)(1) and (2).



(23) (U) In sum, DIVS and its content including results that would also be found in the FBI's CRS would be protected under Exemption (b)(1). It is a classified database deployed with the purpose of facilitating the FBI in carrying out its national security mission. DIVS and its contents are intelligence sources and methods, and would be eligible for protection under Exemption 1; therefore, even if the FBI were able to locate information about individuals in response to a FOIA/PA request, that information would be classified as its contents would reveal

details about an intelligence source and method. Thus, DIVS and its contents would fall squarely within the meaning of §1.4(c).

B. Exemption (b)(3) - Information Protected By Statute National Security Act of 1947 - 50 U.S.C. § 3024 (i)(1)

(24) (U) In addition to FOIA Exemption (b)(1), DIVS contents cannot be released by law per Exemption (b)(3). FOIA Exemption (b)(3) exempts from disclosure information that is specifically protected by statute…"provided that such statute (A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue and (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld." *See* U.S.C. § 552 (b)(3). In this particular case, the FBI would assert Exemption (b)(3) to protect information pursuant to Section 102(A)(i)(1) of the National Security Act of 1947 ("NSA"), as amended by the IRPTA, 50 U.S.C. § 3024 (i)(1), which provides that the Director of National Intelligence ("DNI") "shall protect from unauthorized disclosure intelligence sources and methods."[7] *See* 50 U.S.C. § 3024 (i)(1). As relevant to U.S.C. § 552 (b)(3)(B), the National Security Act of 1947 was enacted before the date of enactment of the OPEN FOIA Act of 2009. On its face, this federal statute leaves no discretion to the DNI about withholding from the public information about intelligence sources and methods. Thus, the protection afforded to intelligence sources and methods by 50 U.S.C. § 3024(i)(1) is absolute. See CIA v. Sims, 471 U.S. 159 (1985). To fulfill its obligation of protecting intelligence sources and methods, the DNI is authorized to establish and implement guidelines for the Intelligence Community ("IC") for the classification of information under applicable laws, Executive Orders, or other Presidential Directives, and for access to and dissemination of intelligence. 50 U.S.C. §

[7] (U) Section 1024(i)(1) of the National Security Act was previously codified at 50 U.S.C. § 403(i)(1). As a result of the reorganization of Title 50 of the U.S. Code, Section 102A(i)(1) is now codified at 50 U.S.C. § 3024(i)(1).

3024(i)(i)(1). The FBI is one of 17 member agencies comprising the IC, and as such must protect intelligence sources and methods.

(25) (S//NF) [redacted]

C. **Exemption (b)(7)(E)**
Investigative Techniques and Procedures

(26) (U) In addition to FOIA Exemptions (b)(1) and (b)(3), DIVS and its contents

would also receive protection under Exemption (b)(7)(E). FOIA Exemption (b)(7)(E) provides protection for law enforcement information that "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." *See* 5 U.S.C. § 552 (b)(7)(E).

(27) (U) The FBI asserts Exemption (b)(7)(E) to protect information which contains internal and highly sensitive investigatory techniques and procedures authorized for use and utilized by the FBI in law enforcement investigations. This exemption affords categorical protection to techniques and procedures used in law enforcement investigations or prosecutions; it protects techniques and procedures not well-known to the public as well as non-public details regarding the use of well-known techniques and procedures. In fact, as DIVS is itself both an intelligence source and method and a sensitive investigative technique used by the FBI, the FBI would neither confirm nor deny the existence of any records in DIVS with respect to any individual. The mere revelation, in and of itself, that a DIVS search uncovered records about any given individual would tell a FOIA requester whether they may or may not be of investigative interest to the FBI. This fact alone that the use of this investigative tool located information about an individual would be a key piece of information that could readily be used by criminal elements or terrorists to verify whether they or members of their group are of interest to the FBI. As such, in a manner similar to the FBI's response to requests concerning any individuals connection to a government watchlist, a FOIA Exemption 7(E) *Glomar* would be employed in response to a request for the existence of an individual in DIVS. *See* First Hardy Declaration at ¶¶ 38-44. Confirming any DIVS related records about an individual reasonably could be expected to compromise investigative operations as well as endanger sources and

methods. Specifically confirming that information about any particular individual was, or was not located in DIVS could heighten an individual's suspicion, inducing him or her to more closely scrutinize activities and associations, which in turn would compromise highly sensitive methods and sources. The public disclosure of which could reasonably be expected to risk circumvention of the law.

(28) (U) Even if a Glomar response were not utilized, any information would still remain exempt under 7E. Revealing the contents of any information located within DIVS, would reveal specific details about the use and function of these techniques, the potential targets of the techniques, and the nature of the information collected would enable individuals and terrorist groups to avoid detection by developing countermeasures that would render the technique useless. Release of this type of information could enable subjects of investigations to educate themselves about the use of these techniques and develop countermeasures to circumvent or negate the effectiveness of these techniques. Thus, DIVS and its contents would be exempt from disclosure under FOIA Exemption (b)(7)(E).

III. HARM ANALYSIS

(29) (U) It is important for the Court to consider the immense harms likely to occur should the function of DIVS drastically expand from its intended purpose as an intelligence-gathering database to a FOIA tool. The harms have been examined under the national security and law enforcement perspectives, and are explained in detail below.

a. National Security and Law Enforcement Perspective

(30) (S) [redacted]

(31) (U) Using DIVS as a FOIA tool also exposes the strengths and weaknesses of other government agencies within the Intelligence Community ("IC"). DIVS is comprised of data voluntarily provided to the FBI by various government agencies within the Intelligence and Law Enforcement Communities. *See* Operational Declaration at ¶ 4. Searching and releasing DIVS' information will have an enormous impact on the IC's ability to conduct national security investigations similar to those harms and concerns discussed in ¶ 28. It would also divulge how

the FBI and the IC as a whole collect, process, and use intelligence data. *See* Operational Declaration at ¶ 10. Using DIVS in this manner would have a widespread impact hampering the federal government's ability to protect our nation from future terrorist attacks.

(32) (U) Lastly, the success of DIVS relies on the voluntary contributions of other government agencies. Using DIVS as a FOIA tool would cause government agencies to hesitate or refuse to contribute important intelligence information fearing it could be disclosed in response to a FOIA request. Many government agencies would likely avoid the risk and opt not to contribute critical information. A reduction in intelligence data would have a devastating impact on the FBI's ability to effectively "connect the dots," and conduct national security and law enforcement investigations.

CONCLUSION

(33) (U) DIVS is an intelligence tool that allows the FBI to examine relationships among various items of interest and to make connections across large amounts of data. This intelligence-gathering system and analytical tool is used in national security and law enforcement investigations. Most significantly, using DIVS as a FOIA tool would have a devastating impact on the FBI's investigative efforts. In addition, the FBI has demonstrated that a search of DIVS would be unreasonably burdensome because its use as a FOIA search mechanism is incompatible with its function and design; it expands the scope of the FBI's search obligations beyond those required by FOIA; the search would generate a large number of false positives; and it poses an unreasonable administrative hardship. Moreover, if DIVS was searched, the FBI has demonstrated that disclosure of the system and its contents would be prohibited under executive order (Exemption 1), statute (Exemption 3), and pursuant to FOIA Exemption (b)(7)(E). Lastly, the FBI has detailed the harms to our national security and law enforcement investigations.

~~SECRET//NOFORN~~

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed this 13th day of April, 2015.

DAVID M. HARDY
Section Chief
Record/Information Dissemination Section
Records Management Division
Federal Bureau of Investigation
Winchester, VA