



Department of Energy
Richland Operations Office
P.O. Box 550
Richland, Washington 99352

October 30, 2015

CERTIFIED MAIL

Mr. Nikolas Peterson
Hanford Challenge
219 First Avenue South
Suite 310
Seattle, Washington 98104

Dear Mr. Peterson:

FREEDOM OF INFORMATION ACT REQUEST (FOI 2016-00015)

This letter is in response to the electronic Freedom of Information Act (FOIA) request you submitted to the U.S. Department of Energy (DOE) Headquarters FOIA Office on September 1, 2015, requesting "the document(s) titled (either specifically or similarly to): Federal Occupational Health Initial Assessment for Electronic Medical Record System, dated on or about August 20, 2015 (8/20/2015), and in possession by the Department of Energy." In a letter to you dated October 13, 2015, this office notified you that since the requested document was generated by another Federal agency, the U.S. Department of Health and Human Services (HHS), your request was transferred to the FOIA Officer at that location for a release determination. Since that time, HHS requested DOE make the release determination and provide the response directly to you.

We have interpreted your request for a copy of the enclosed document entitled "Initial Assessment of Electronic Medical Records System" generated by Federal Occupational Health (FOH). If our interpretation of your request is incorrect, please contact this office.

The document is enclosed with certain deletions pursuant to Exemptions 5, 6 and 7E of the FOIA. Exemption 5 protects "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. This Exemption protects those documents normally privileged in the civil discovery process, such as pre-decisional, deliberative process material. The deliberative process protects advice, recommendations, and opinions that are pre-decisional and part of the decision-making process of the Government. This privilege protects not merely the documents, but also the integrity of the deliberative process itself where the exposure of that process, or an element thereof, would result in harm. It is reasonably foreseeable that release of such information could chill open and frank discussions, limit government personnel's range of options to consider, and thus detract from the quality of Agency decisions.

We also withheld the name of the employee interviewed on page 5 pursuant to Exemption 6. Exemption 6 provides that an agency may protect from disclosure all personal information if its disclosure would constitute a clearly unwarranted invasion of privacy by subjecting the individuals to unwanted communications, harassment, intimidation, retaliation, or other substantial privacy invasions by interested parties.

In invoking Exemption 6 we considered 1) whether a significant privacy interest would be invaded by disclosure of information, 2) whether release of the information would further the public interest by shedding light on the operations or activities of the government, and 3) whether in balancing the private interest against the public interest, disclosure would constitute a clearly unwarranted invasion of privacy. We have determined that the public interest in the identity of the individual whose name appears in the document does not outweigh the individual's privacy interests.

Lastly, Exemption 7(E) provides that, "records or information compiled for law enforcement purposes" may be withheld from disclosure, but only to the extent that the production of such documents "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."

Sensitive information about DOE networks, systems, and communications has been withheld pursuant to Exemption 7(E). The withheld information pursuant to Exemption 7(E) includes, but is not limited to, preventative law enforcement and/or security purposes to prevent future illegal acts in the form of cyber security intrusions, and investigative techniques that could be used to obtain classified or sensitive information on DOE networks without authorization. This report includes specific system vulnerabilities and if released, could compromise DOE's cyber security posture and ability to protect sensitive information.

This satisfies the standard set forth by the Attorney General by Memorandum on March 19, 2009, that the agency is justified in not releasing material that it reasonably foresees that disclosure would harm an interest protected by one of the statutory exemptions or disclosure is prohibited by law. This also satisfies DOE's regulation at Title 10, Code of Federal Regulations (CFR), Section 1004.1, to make records available which it is authorized to withhold under 5 U.S.C. 552 when it determines that such disclosure is in the public interest. Accordingly, we will not make discretionary disclosure of this information.

All releasable information in the documents has been segregated and is being provided to you. The undersigned individual is responsible for this determination. You have the right to appeal to the Office of Hearings and Appeals, as provided in 10 CFR 1004.8. Your appeal shall be filed within 30 days after receipt of this letter. You may submit your appeal by e-mail to OHA.filings@hq.doe.gov, including the phrase "Freedom of Information Appeal" in the subject line. Alternatively, any such appeal may be made in writing to the following address: Director, Office of Hearings and Appeals (HG-1), U.S. Department of Energy, L'Enfant Plaza Building, 1000 Independence Avenue SW, Washington, D.C. 20585-1615. Should you choose to appeal, please provide this office with a copy of your e-mail or letter.

Mr. Nickolas Peterson

-3-

October 30, 2015

If you have any questions regarding your request, please contact me at our address above or on (509) 376-6288.

Sincerely,

-Original Signed By-

Dorothy Riehle
Freedom of Information Act Officer
Office of Communications
and External Affairs

OCE:DCR

Enclosure

FEDERAL OCCUPATIONAL HEALTH

DEPARTMENT OF ENERGY

HANFORD SITE,
RICHLAND WASHINGTON

INITIAL ASSESSMENT OF
ELECTRONIC MEDICAL RECORD SYSTEM

CURRENT STATE

Dated: 8/20/2015



Table of Contents

1. Background.....	3
2. Scope of the Assessment	4
3. Risk Definition	5
4. Issues with Current State	7
5. Recommendations	12
Appendix A: FIPS Minimum Security Requirements.....	13
Appendix B: FIPS and FISMA Reference Information	16
Table 1: Risk Categorization Legend.....	6
Table 2: Summary of Issues by Risk Category.....	6
Figure 1: (b)(5) Current State of DOE Hanford OHM	4



1. Background

The Department of Energy (DOE) organization located in Richland, WA is responsible for providing medical clearance and surveillance examinations for an estimated 12,000 contractor individuals whose role is to support DOE's mission for the Hanford site. The DOE maintains two (2) health clinics in the area. One is located at the Hanford site and the other is located in an office building in Richland, WA. Each clinic performs approximately 15-20 occupational examination related visits each business day and some on Saturday. At the current time, HPM Corporation (HPMC) is the contractor who operates the clinics and also supports the technical platform chosen to manage examination and clearance data.

The following schematic depicts the systems in use today for this purpose and is the object of this initial assessment. The PeopleCore system stores and maintains person demographic data and provides contractor records to the Employee Job Task Analysis (EJTA) and DOE's electronic medical record system Occupational Health Management (OHM) built by United Labs. The EJTA system is an electronic questionnaire that generates the physical and medical clearance/surveillance requirements for an individual and is used within the OHM system. The PeopleCore system is built upon the PeopleSoft HR software. The EJTA system is a custom-built application, which is approximately 20 years old, while the OHM application is customized version of PureSafety, a commercial off-the-shelf (COTS) product offered by United Labs (UL).

The schematic below demonstrates the current state (b)(5)



DOE-Hanford Current State (b)(5)

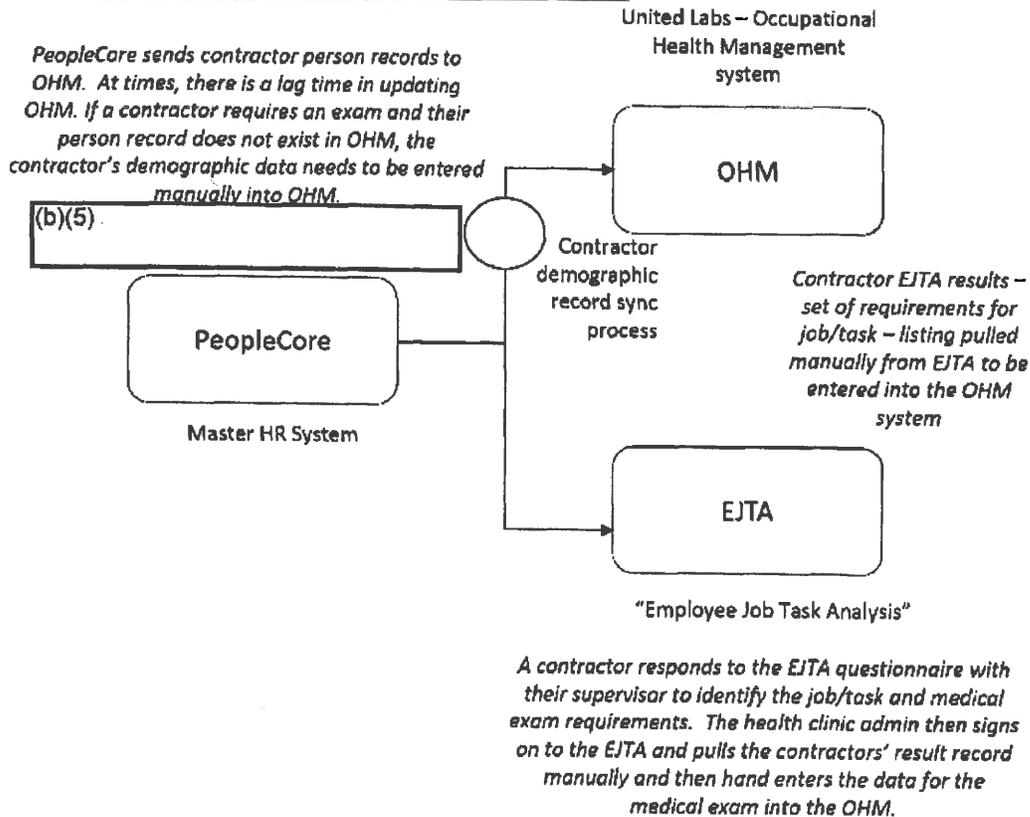


Figure 1: (b)(5) Current State of DOE Hanford OHM

Currently, the DOE has options related to the maintenance and upgrade of the EJTA system because of its age and the inability to interconnect with the OHM. One viable option is to

(b)(5)

(b)(5)

An alternative is (b)(5)

(b)(5)

in addition, DOE may also (b)(5)

(b)(5)

These possibilities are currently being considered by the DOE.

2. Scope of the Assessment

The DOE requested that FOH perform a cursory assessment of their electronic medical record software, OHM, in its current state. The contractor supporting this software is HPMC. While this contractor (b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

DOE elected to request an immediate, independent analysis of the technology.



Diane Mauk, software architect and senior consultant with FOH, visited the DOE Hanford offices Monday, August 3 through Wednesday, August 5, 2015. During this visit, Diane met with several members of the HPMC contracting company, and participated in meetings to learn about the software architecture, infrastructure, dependent systems as well as union policies and directives. HPMC provided a tour of the health clinic, a description of the employed business practices as well as the use of OHM in the clinical setting. Diane was able to speak with a physician (b)(6) a nurse, and a case worker. A walkthrough of the software and the known defects was presented by the HPMC contractor who is responsible for managing and implementing the changes/fixes to OHM. Other discovery meetings were conducted with the DOE IT management who are federal employees. Beyond the aforementioned parties, no interviews were conducted with DOE unionized contract employees that receive clinical services from the onsite clinics.

This document is an initial assessment of the findings from the visit to the DOE Hanford office, as well as the OHM software product. In addition, the Employee Job Tasking Analysis (EJTA) system was included in the overall assessment (b)(5)

(b)(5)

At the end of the assessment period, (b)(5) out-brief was provided to DOE Hanford office executive management, which described (b)(5)

(b)(5)

3. Risk Definition

This document describes the most noteworthy issues discovered during the initial assessment and how (b)(5)

(b)(5)

(b)(5)

issues. In particular, the following legend is used to (b)(5) documented below.

Legend	Risk Category
(b)(5)	

Table 1: Risk Categorization Legend

Of the 10 major issues documented below, the following table provides a summary of the total

(b)(5)

Legend	Total Issues Associated with Risk Category
(b)(5)	
(b)(5)	
(b)(5),(b)(7)(E)	
(b)(5)	

Table 2: Summary of Issues by Risk Category



4. Issues with Current State

Issue # 1	(b)(5)
(b)(5)	
Risk Impact	(b)(5)
Risk Category	(b)(5)



Issue # 2	(b)(5),(b)(7)(E)
(b)(5),(b)(7)(E)	
Risk Impact	(b)(5),(b)(7)(E)
Risk Category	

Issue # 3	(b)(5)
(b)(5)	
Risk Impact	(b)(5)
Risk Category	



Issue # 4	(b)(5),(b)(7)(E)
(b)(5),(b)(7)(E)	
Risk Impact	(b)(5),(b)(7)(E)
Risk Category	

Issue # 5	(b)(5),(b)(7)(E)
(b)(5),(b)(7)(E)	
Risk Impact	(b)(5),(b)(7)(E)
Risk Category	



Issue # 6	(b)(5),(b)(7)(E)
(b)(5),(b)(7)(E)	
(b)(5),(b)(7)(E)	There are no records of any of the changes made to the system for some months in 2013 and all of 2014. (b)(5),(b)(7)(E)
(b)(5),(b)(7)(E)	
Risk Impact	(b)(5),(b)(7)(E)
Risk Category	

Issue # 7	(b)(5)
(b)(5)	
Risk Impact	(b)(5)
Risk Category	

Issue # 8	(b)(5)
(b)(5)	
Risk Impact	(b)(5)
Risk Category	

Issue # 9	(b)(5)
(b)(5)	
Risk Impact	(b)(5)
Risk Category	

Issue # 10	(b)(5)
(b)(5)	
Risk Impact	(b)(5)
Risk Category	

5. Recommendations

Due to the (b)(5) (b)(5) the following (b)(5) recommendations are proposed based on this initial assessment:

1) Consider (b)(5) (b)(5)

2) Consider (b)(5) (b)(5)

3) Consider (b)(5) (b)(5)

(b)(5)

If the DOE wishes to (b)(5) it is recommended that (b)(5)

(b)(5)

Appendix A: FIPS Minimum Security Requirements

The following is a list of the FIPS minimum security requirements and an inclusion/exclusion statement regarding this initial assessment. Please refer to NIST FIPS Publication 200 for more detailed information.

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E) Initial Assessment Findings: (b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E) Initial Assessment Findings: Not included in initial assessment

(b)(5),(b)(7)(E)



(b)(5), (b)(7)(E) Initial Assessment Findings: (b)(5), (b)(7)(E)
(b)(5), (b)(7)(E) The DOE IT managers stated (b)(5), (b)(7)(E)
(b)(5), (b)(7)(E)
(b)(5), (b)(7)(E)

(b)(5), (b)(7)(E) Initial Assessment Findings: The DOE IT managers stated (b)(5), (b)(7)(E)
(b)(5), (b)(7)(E)
(b)(5), (b)(7)(E)

(b)(5), (b)(7)(E) Initial Assessment Findings: (b)(5), (b)(7)(E)
(b)(5), (b)(7)(E)
(b)(5), (b)(7)(E)

(b)(5), (b)(7)(E) Initial Assessment Findings: (b)(5), (b)(7)(E)
(b)(5), (b)(7)(E)

(b)(5), (b)(7)(E) Initial Assessment Findings: This was not included in the assessment.

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

Initial Assessment Findings: This was not included in the assessment.

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

Initial Assessment Findings: Because the HLAN and other systems are maintained by Lockheed Martin, this was not included in the assessment.

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

Initial Assessment Findings: This was not included in the assessment.

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

Initial Assessment Findings: This was not included in the assessment.

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

Initial Assessment Findings: This was included in the assessment and provided in the content above.

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

Initial Assessment Findings: This was not included in the assessment.

(b)(5),(b)(7)(E)



(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

Initial Assessment Findings: This was not included in the assessment.

(b)(5),(b)(7)(E)

(b)(5),(b)(7)(E)

Initial Assessment Findings: This was not included in the assessment.

Appendix B: FIPS and FISMA Reference Information

"FIPS 200 AND FISMA NIST SP 800-53 IMPLEMENTING INFORMATION SECURITY STANDARDS AND GUIDELINES FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, is a mandatory federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53. This allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation. FIPS 200 and NIST Special Publication 800-53, in combination, ensure that appropriate security requirements and security controls are applied to all federal information and information systems. An organizational assessment of risk validates the initial security control selection and determines if additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of security due diligence for the organization."

An excerpt from National Institute for Standards and Technology (NIST) Special Publication 800-53 Revision 4 -- Security and Privacy Controls for Federal Information Systems and Organizations

