Privacy Impact Assessment

for the

Biological Detection for the 21st Century (BD21) Technology Demonstration (TD)

DHS Reference No. DHS/CWMD/PIA-002

July 6, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Countering Weapons of Mass Destruction (CWMD) Systems Support Directorate has been tasked and funded to evaluate networked biological detection and presumptive identification equipment for the purposes of informing the next generation detection of airborne bio-threats, as well as to recapitalize the BioWatch Program.[1] To fulfill these responsibilities, CWMD is developing the Biological Detection for the 21st Century (BD21) Program. CWMD will install biological detection equipment at certain locations/sites as sensor nodes in various configurations. Each node is comprised of biological sensors, Global Positioning System (GPS) technology, a communications unit, meteorological sensors, and cameras, which are monitored and operated remotely (where possible). The sensor nodes capture environmental data and camera video/images which are transmitted to CWMD's secure Amazon Web Services (AWS) Cloud for the purpose of developing algorithms and evaluating performance of the technologies. CWMD is conducting this PIA to evaluate the privacy risk associated with the use of this technology.

Introduction

BD21 is a CWMD major acquisition program pursuing a next-generation capability to detect airborne bio-threats. The BD21 Program concept incorporates anomaly detection, response personnel communication, and situational awareness to Federal, State, and Local stakeholders to ensure appropriate and timely actions can be taken to mitigate the consequences of a biological incident/attack. As the BD21 Program is early in the DHS Acquisition Lifecycle Framework, it is focused on executing Alternatives Analysis, conducting Technology Maturity Assessments, and establishing operational requirements and Concept of Operations (CONOPS). In order to inform these activities, the BD21 Technology Demonstration (BD21 TD) has been established. Its purpose is to collect environmental, system performance, cost, and capability data on similar types of systems that may comprise components of the eventual BD21 platform. The overall objective of CWMD's research efforts is not to collect personally identifiable information (PII), but to understand how the biological sensor technologies perform and ultimately could facilitate CWMD operations.

The BD21 TD technologies being evaluated have the potential to be a valuable tool for situational awareness and rapid response in the event an aerosolized biological threat agent is released. The sensor nodes are a means to collect and transmit environmental and equipment performance data to CWMD. They are equipped with cameras that store and feed images/video directly to the CWMD's secure AWS cloud. The imagery is used to confirm the reliability of the biological equipment (e.g., did the equipment alert because of a threat or benign event/interferent).

[1] More information about the BioWatch Program is available at: https://www.dhs.gov/biowatch-program.

The scope of the current BD21 TD research will include an ongoing evaluation of the outdoor environment located at The World Trade Center and the indoor environments at Newark Airport and Grand Central Terminal in New York City over the next several years.[2]

Demonstrating/evaluating the biological sensors for CWMD mission sets typically requires high population centers and/or high traffic locations. Cameras provide the means of confirming the performance of the technologies by collecting images/information that will provide situational awareness in proximity of the sensor node. For example, it is of interest if natural (e.g., weather) or man-made (e.g., trucks/cars) factors cause a certain sensor to alert. This project does not require PII collection. Any inadvertent images captured will not be used to identify individuals, nor are there plans to use facial recognition technology.

Nonetheless, CWMD will take all reasonable steps necessary to maintain the security of any potential PII, and will protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. All of the data that is initially captured at the sensor nodes will be used for research exercises and can only be accessed and disseminated by a few select individuals within the BD21 Program.

The BD21 Program will use two types of video/image collection techniques. Cameras can capture data in approximately 4-minute snippets on either side of an alert and as continuous footage.

For camera footage captured in 4-minute snippets around an instrument alerting, the footage is temporarily saved on an external hard drive as well as transmitted (encrypted) to the CWMD AWS Cloud for storage. The video snippets are uploaded to AWS only after a triggered alarm. For footage collected continuously, the data is saved temporarily on an external hard drive, and in some cases an SD card (if the unit contains an Optical Warning and Localization (OWL) communications unit/system). The SD card contained within the OWL deletes its footage automatically after 16 hours and is not removed. The external hard drives for the continuous footage collection are removed at specified intervals (e.g., on a monthly basis). Once the continuous raw video footage is transferred from the external hard drives to an onsite storage, they are cleared and returned to the sensor node site.

The CWMD AWS Cloud and any on-site storage have access controls in place that ensure only those with an authorized need to know can access data. When possible, files are further protected with permissions that are separate from an individual's normal login accounts. According to the BD21 Data Management Plan, upon completion of the CWMD AWS Cloud System Authorization Access Request form, specific trainings, and approval from the CWMD AWS Cloud System Owner, a user account is created. In cases where the data is sent or access is granted to an end user, appropriate precautions are taken for context, data use, and security of both

[2] Additional public locations similar to these may be planned in the future.

the specific data transfer and the overall integrity of the system. Personnel also need special account provisioning from the BD21 Anomaly Detection Algorithm Technical Lead to access any on-site stored data. The current user base of those with access is small to ensure appropriate safeguarding of data.

The data collected from the BD21 TD sensor nodes will not be maintained in a manner that allows it to be linked to any other types of PII. CWMD will minimize the use and sharing of camera footage. Should any of the images/video be selected for use in a briefing/presentation/report, CWMD will ensure faces are blurred/removed and ensure the appropriate markings and security have been addressed.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[3] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[4]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[5] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[6] and the Homeland Security Act of 2002, Section 222.[7] Given that CWMD BD21 TD is a research project rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This PIA examines the privacy impact of the BD21 TD as it relates to the Fair Information Practice Principles.

[3] 5 U.S.C. § 552a.
[4] 6 U.S.C. § 142(a)(2).
[5] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[6] 44 U.S.C. § 3501 note.
[7] 6 U.S.C. § 142.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

The BD21 Program will only place devices in public locations where individuals have no expectation of privacy (e.g., areas with unrestricted access at major transportation hubs). This PIA also provides a level of transparency to the public regarding CWMD BD21 demonstration efforts. This project does not require the collection of PII. Any inadvertent images captured will not be used to identify individuals, nor will facial recognition technology be used. CWMD programs and projects will take all reasonable steps necessary to maintain the security of any potential PII collected incidentally and will protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. The BD21 Team will minimize the use and sharing of camera footage. For example, if images/video are selected for use in a briefing/presentation/report, the BD21 Team will ensure that faces of individuals captured will be blurred/removed and that appropriate markings and security requirements have been addressed.

Privacy Risk: There is a risk that individuals will not know their images may be captured by BD21 devices.

Mitigation: This risk is partially mitigated. This PIA and other CWMD and BD21-specific information provide the public some level of transparency about this type of CWMD mission. However, providing direct notice to all individuals who may be captured in footage is not feasible. CWMD mitigates the impact of collecting images inadvertently without providing notice by not linking those images to any other types of PII or a specific individual.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

The video and images obtained will be used primarily to enhance overall situational awareness around the perimeter of the sensor node. This data will be used further to develop algorithms and evaluate performance of the technologies informing the next generation detection of airborne bio-threats.

This project does not require the collection of PII. Any inadvertent images captured during the demonstrations will not be used to identify individuals. Because of the nature of this program, there is generally no way for individuals to consent to their images being inadvertently captured. However, the BD21 Team only places cameras in public locations where individuals have no expectation of privacy (e.g., the unrestricted access areas of major transportation hubs). Nonetheless, CWMD programs and projects will take all reasonable steps necessary to maintain

the security of any potential PII, and will protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction.

Given that no images or data will be associated with a single individual, no specific redress mechanisms are warranted. However, individuals seeking redress may submit a request in writing to the DHS Chief Privacy and Freedom of Information Act (FOIA) Officer at the address below, or to the respective Component's FOIA officer, which can be found at https://www.dhs.gov/foia-contact-information. DHS also allows Privacy Act and FOIA requests to be submitted electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form.

Chief Privacy Officer and Chief Freedom of Information Act Officer
Privacy Office, Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The Countering Weapons of Mass Destruction Act of 2018[8] established CWMD as the DHS Component responsible for efforts and coordination with domestic and international partners to safeguard the United States against chemical, biological, radiological, nuclear, and health security threats. The BD21 TD's purpose is to collect environmental, system performance, cost, and capability data on similar types of systems that may eventually be a part of the operational BD21 platform to detect and/or prevent airborne bio-threats. Cameras provide the means for collecting images/information that will help CWMD better understand the technologies under evaluation (e.g., additional situational awareness and what causes certain technologies to alert). This project does not require PII collection.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The BD21 Program only deploys cameras as a situational awareness/contextual data tool to support the evaluation of the biological sensor equipment. The video/images collected are necessary in furtherance of that evaluation to understand, for example, if natural (e.g., weather) or man-made (e.g., trucks/cars) factors cause a certain sensor to alert. Details of the environment at the time a sensor alerts will help CWMD develop algorithms and evaluate performance of these technologies that will inform next generation detection of airborne bio-threats. Further, the

[8] Countering Weapons of Mass Destruction Act of 2018, Pub. L. 115-387 (December 21, 2018).

cameras deployed are not meant to capture enough detail to identify individuals or conduct facial recognition. Video footage will only be used to confirm equipment alerts/alarms and never be matched to any other PII.

While there is no direct intention/need to collect PII for this project, CWMD will be mindful of the information's sensitivity and take all reasonable steps necessary to maintain the security of any potential PII, and will protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction.

Information collected is deleted from the camera external hard drives once uploaded to the secure CWMD AWS Cloud or on-site storage. The video footage will be retained (likely three to four years) to understand the performance of the respective technologies and the development of the R&D algorithm. Once the images/video are no longer needed during the research phase, they will be disposed of in accordance with proper DHS destruction requirements.

Privacy Risk: There is a risk that more information is collected than required.

Mitigation: This risk is partially mitigated. CWMD needs to maintain all available information from the sensor nodes in order to establish baseline understanding of the technology, as well as factors that cause the sensor nodes to trigger. The other metadata, in additional to the image/video data that is collected, will help the BD21 Program determine the feasibility of operationalizing biological detection technologies. Any image/video captured during the demonstrations will not be used to identify individuals.

Privacy Risk: There is a risk that CWMD will maintain more information than is necessary for longer than is required.

Mitigation: This risk is partially mitigated. It is standard practice for research programs to maintain data for the life of the project, which is expected to be three to four years in this instance. CWMD has determined that is necessary for the research phase of the BD21 Program, which will ensure CWMD has all available measurements to determine the feasibility of operationalizing these biological detection technologies. Although CWMD will maintain inadvertent images/video through its sensor node cameras, this information is not associated with specific individuals.

As the BD21 Program nears the end of this research phase, it will reassess the length of time needed to maintain the data it receives from the sensor nodes.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Information will only be used to assess the respective technologies under evaluation. Their capability to accurately and quickly detect and identify biological threat agents is key to evaluating

the systems. The camera footage allows the BD21 Team to observe if technologies are performing as expected and meeting CWMD's operational mission requirements.

Observations and research analysis data may be shared with federal, state, and local partners, but the BD21 Team will minimize the use of images considered PII data (i.e., faces of individuals) before sharing. If the images/video are important in conveying findings, such as in briefings, the portions considered PII will be masked and/or blurred for an individual's protection.

Data can be shared to partners through direct or indirect access. Regarding direct access, the BD21 Team can set up user accounts allowing partners to access relevant BD21 Program data directly within the CWMD AWS Cloud environment. Regarding indirect access, when the BD21 Team is unable or it is inappropriate to provide direct access, data is properly protected according to applicable security requirements, then sent through secure file transfer protocol (SFTP) to partners.

Partners may include:

- Massachusetts Institute for Technology - Research & Development contractor that is developing the anomaly detection algorithm;
- SAIC - Test & Evaluation contractor that is testing the algorithm;
- Department of Defense Joint Program Executive Office (JPEO) as an external collaborator/partner with its own existing sensor network; and
- Defense Advanced Research Projects Agency SIGMA+ as an external collaborator/partner with its own existing sensor network.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Information collected will only be used to assess the biological sensor equipment. The video and images generated by the sensor nodes are only used to evaluate the system. There is no specific need for PII to be collected to perform the assessment of the technologies. Any PII collected would be inadvertent and would hold no value for the BD21 Program, so it would be incongruous to take steps to improve or maintain the quality and integrity of PII data when that data is undesirable. The images provide situational awareness and confirm a respective technology's alert, they are not intended and will not be used to capture PII.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

CWMD will adhere to the security safeguards that govern all DHS and CWMD operations as it would during any research effort. Any images/video captured by the sensor nodes will be deleted/overwritten from the hard drives/SD cards and stored within the cloud or on-site locations. Only those individuals with an authorized need to know will have access to the sensor node components/AWS Cloud/storage locations and the information contained therein.

Privacy Risk: There is a risk that unauthorized individuals may access the data.

Mitigation: This risk is mitigated. CWMD programs and projects will take all reasonable steps necessary to maintain the security of all data collected, and will protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. The CWMD AWS Cloud has access controls in place that ensure only those with an authorized need to know can access images and other data associated with the BD21 Program. User accounts are only provisioned upon completion of the CWMD AWS Cloud System Authorization Access Request form, specific trainings, and approval from the CWMD AWS Cloud System Owner. All camera images/video captured by the sensor nodes during the demonstration are transmitted to secure hard drives (later deleted) and then CWMD's secure AWS Cloud or on-site locations, which can only be accessed by those having a need to know. Any PII collected will be safeguarded along with all other data collected.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

CWMD personnel and all DHS contractors are required to complete annual DHS privacy training regarding the safe handling and protection of PII.

The images/video data captured is only accessible to a few select individuals who must undergo an account provisioning process. Data is deleted from the sensor node hard drives at specific intervals and transferred to the CWMD AWS Cloud or on-site storage for archiving and used by limited number of individuals who have obtained access approval.

Conclusion

Biological detection and presumptive identification technology is a valuable tool for increased situational awareness and rapid response to an airborne biological threat agent. The overall objective of the BD21 TD is not to collect PII, but to provide situational awareness around the installed sensor nodes and confirm the performance the biological technology under evaluation.

Evaluation of biological technologies for CWMD mission sets typically requires public locations which are highly populated areas and/or heavily travelled. All data captured by the sensor nodes is transmitted and ultimately stored within the CWMD AWS Cloud or on-site locations which have technical and administrative controls in place to ensure appropriate access. CWMD will continue to work with the DHS Privacy Office to ensure this program maintains the practices outlined in this PIA and protects individual privacy.

Responsible Official

Ron Major
R&D PM/BD21 Algorithm Development Lead
DHS HQ/CWMD
CWMDbiodetection21@hq.dhs.gov

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717