SYSTEM FOR AUTOMATED BACKGROUND EVALUATION & REVIEW (SABER) PROTOTYPE
STATEMENT OF OBJECTIVES

1.0 BACKGROUND

The Office of the Under Secretary of Defense for Intelligence (OUSD(I)) and the Defense Security Service (DSS) are responsible for vetting and managing security clearances for civilian government, military, and contractor personnel affiliated with the Department of Defense (DoD). Today, this process is spread across multiple federal agencies and has led to a series of overburdened queues, opaque and disjointed processing, and an on average 13-month turnaround for cases.

In the coming months, as the National Background Investigation Bureau (NBIB) realigns under DSS, the DoD will assume responsibility for all parts of this mission: classification, investigation, adjudication, and continuous vetting. This will require significant effort to replace and streamline multiple critical information systems that manage and augment Subject data throughout the process.

The Defense Digital Service (DDS), in coordination with OUSD(I), will direct the creation of a prototype system that successfully collects a Subject's information, executes a background investigation (with automated and manual parts), and records an adjudication decision. This prototype will require integration with a wide variety of U.S. Government and commercial databases to verify the Subject's identity and background information. Development of the prototype will be rapid and agile in nature, fielding new functionality to users for feedback every two weeks.

This project will be executed in a manner consistent with best practices from the Digital Service Playbook[1] and the TechFAR Handbook[2]. The vendor will provide a cross-functional team of software engineers, user researchers, designers, and product managers to drive the repeatable process for the delivery of a functional software prototype.

1.1 DEFINITIONS

Adjudicators: DoD employee responsible for evaluating a background investigation case and issuing a decision regarding an individual's fitness for federal service, based on established suitability and security standards.
DDS: Defense Digital Service
DSS: Defense Security Service
DoD: U.S. Department of Defense

1 https://playbook.cio.gov/
2 https://playbook.cio.gov/techfar/

Investigators: DoD employee or contractor responsible for obtaining and verifying details about a Subject's background and other information relevant to their fitness for federal service
MVP: Minimum Viable Product
NBIB: National Background Investigation Bureau
ODNI: Office of the Director of National Intelligence
OPM: Office of Personnel Management
OUSD(I): Office of the Under Secretary of Defense for Intelligence
Subject: Applicant for federal employment and/or a security clearance

2.0 APPLICABLE DOCUMENTS

- Public Law 90-629, Arms Export Control Act, dated 26 Dec 2013
- EO 12470 or the Arms Export Control Act, Continuation of Export Control Regulations, dated 30 Mar 1984
- DoD Directive 5230.25 Withholding of Unclassified Technical Data from Public Disclosure, 6 Nov 1984 Incorporating Change 1, dated 18 Aug 1995
- Section 508 of the Rehabilitation Act of 1973
- DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)
- NIST Special Publication 800-37
- Homeland Security Presidential Directive 12

3.0 ACQUISITION PROCESS

3.1 Request for White Papers (RWP) Circulation

The Defense Digital Service is seeking interested vendors to submit white papers in response to the needs addressed in this Statement of Objectives. Interested vendors should prepare a response, no more than ten (10) pages including any exhibits or appendices, for submission no later than March 26, 2019 in accordance with the attached template. The Government will confirm receipt of each vendor's white paper within 24 hours of submission; if you do not receive a confirmation in that period, please contact the AO immediately. No submissions will be accepted after the deadline (March 26, 2019) regardless of circumstances.

All vendors with questions must submit the questions, in writing, to the Agreements Officer (see §10) by March 19, 2019. All questions, along with the Government responses, will be published publicly within 48 hours. The Government is unable to answer any questions privately or after these deadlines under Federal law and regulations.

The Government will review white papers and select one or more vendors to continue in the process outlined below.

3.2 Technical Challenge Release

Selected vendors will be provided a Technical Exchange document outlining a technical challenge along with Participation Instructions. The Technical Exchange is intended to function as an in-depth assessment of the vendor's software development capabilities. Vendors will have seven (7) calendar days to complete the technical challenge and submit their code in accordance with the Participation Instructions. The Government will not accept any submissions after the seven (7) calendar day deadline, regardless of circumstances.

The Government will review submitted Technical Challenges and select one or more vendors to continue in the process outlined below.

3.3 Technical Challenge Demonstration and Review

Upon completion of the vendor's technical challenge, the vendors will be invited to the Pentagon to demonstrate their responses/products, and highlight their firm's capabilities in-person to the Selection Team. Vendor interviews will be 90 minutes including questions and answers from the vendors.

3.4 Selection for Negotiation and Request for Proposals

After these demonstrations and interviews, the Government may select one or more vendors to begin negotiations with, and will invite them submit a full proposal, to pricing information.

3.5 Proposal Review, Award, Kickoff

The Government will review the submitted full proposals and may select one or more vendors for contract award. The Government will provide final agreements to the vendor and a start date will be negotiated between the Government and the selected vendor(s).

4.0 VENDOR REQUIREMENTS

4.1 GENERAL REQUIREMENTS

4.1.1 Security: The highest level of classification for this effort is:

☒ **UNCLASSIFIED** ☐ SECRET ☐ TOP SECRET/SCI

4.1.1.1 Information Subject to Export Control Laws/International Traffic in Arms Regulation (ITAR):

Public Law 90-629, "Arms Export Control Act," as amended (22 U.S.C 2751 et. Seq.) requires that all unclassified technical data with military application may not be exported lawfully without an approval, authorization, or license under EO 12470 or the Arms Export Control Act and that such data required an approval, authorization, or license for export under EO 12470 or Arms Export Control Act. For purposes of making this determination, the Militarily Critical Technologies List (MCTL) shall be used as general guidance. All documents determined to contain export controlled technical data will be marked with the following notice:

WARNING: This document contains technical data whose export is restricted by the Arms

Export Control Act (Title 22, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

4.1.2 Data Rights: The deliverables under this OT Agreement will generally be a functional software product. The government may require that the code developed under this project be available for public release as open source software. As such, the Government will negotiate intellectual property terms consistent with this goal, which will anticipate unlimited rights.

4.2 TECHNICAL REQUIREMENTS

Award recipient will build a prototype software product, which addresses the need to consolidate all parts of the personnel vetting and security clearance adjudication process. Award recipient will maintain close communication with DDS throughout the development and sprint planning/review processes, to establish and receive feedback on the requirements for each sprint.

4.2.1 Components

The software prototype must include the following:

Infrastructure:

- Commercial cloud hosting environment at DoD Impact Level 4[3] for Controlled Unclassified Information (CUI)
- Separate development, test, and production environments
- Predictable, scalable, templated virtual environments using commercially available orchestration tools
- Continuous integration/continuous deployment pipeline following commercial best practices
- Commercial best practices for information security, including proper controls for CUI and Personally Identifiable Information (PII)

Process & Transparency:

- Sprint reviews, including Government personnel, on a schedule directed by the AOR
- Government control of and persistent access to source code and application environment
- Consistent use of a source code version control system (e.g. git)
- Occasional demonstrations of the software for the Government

Software:

- Automated unit and integration testing, with over 90% codebase coverage

3 https://iase.disa.mil/cloud_security/cloudsrg/Pages/ImpactLevels.aspx

- Modern programming languages, with sound, documented technical decisions and justifications
- Robust, secure integrations with various U.S. Government and commercial data sources as required by the Government for identity and background information validation
- Configurable business processes, with measurable results
- Appropriate use of applicable Platform-as-a-Service (PaaS) offerings
- Adaptable/compatible with all commercial/Government software and upgrades

Design & Research:

- Development and execution of a user research plan incorporating existing Government-provided research
    - Should include user interviews, storyboards, wireframes, surveys/feedback collection
- User experience and interface design leveraging the U.S. Web Design System[4]
- Consistent collection of feedback against working software through usability testing

Compliance:

- Adherence to the Revised Standards of Section 508 of the Rehabilitation Act of 1973[5], incorporating WCAG 2.0 Level AA success criteria to ensure broad accessibility
- Document security protocols in accordance with commercial best practices. Documentation must be robust enough to address the spirit of the NIST Risk Management Framework (RMF)[6]

The final, shipped prototype is defined as the Minimum Viable Product capable of collecting Subject's information for a specified population, executing a background investigation of a specified type (including automated record checks, deconfliction/entity resolution, and manual investigation notes entry), and recording an adjudication decision which meets the software principles below.

4.2.2 Software Principles:

The prototype must adhere to the following principles:

1. Places the Subject at the center of the process;
2. Improves overall process/system transparency with a focus on Subjects' visibility into the process/system;

4 https://v2.designsystem.digital.gov/
5 https://www.section508.gov/create/applicability-conformance
6 https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

3. Provides significant improvements to user experience, workflow and information management, and productivity for additional non-Subject user communities (e.g. investigators, adjudicators, evaluators);
4. Significantly shortens the lifespan of an investigation and adjudication;
5. Facilitates Subjects' enrollment in Continuous Evaluation;
6. Supports the DoD's expanded personnel vetting mission; and
7. Allows for experimentation of the business processes around the background investigation process.

4.2.3 Authority to Operate:
The vendor shall deliver a complete, working software product that is capable of receiving a favorable Authority to Operate decision, following a streamlined process defined by the Government during the development process .

4.3 REPORTING REQUIREMENTS

4.3.1 Regular Agile Reporting: The vendor shall participate in typical agile ceremonies and provide associated artifacts following each sprint to include release notes, burndown/burnup charts, and sprint retrospectives. All system improvements, including source code, must be documented and openly available to DDS.

4.3.2 Incident Reporting: The vendor shall immediately notify the AOR and any previously designated Government security contacts in the event that the vendor determines that a unauthorized access has occurred to the production infrastructure, that production information has been spilled onto test or development environments, or of a loss-of-control over production information (including both deletion and compromise). If necessary, the vendor shall assist in the preparation of a Breach of Personally Identifiable Information report (DD 2959). When determining whether or not a reportable event has occurred, the burden of proof shall be reasonable suspicion.

5.0 PERIOD OF PERFORMANCE:

The base period of performance is nine (9) months.
Pursuant to 10 USC 2371b, offerors are notified that a follow-on production OT is possible upon completion of the prototype.

6.0 PLACE OF PERFORMANCE

Vendor facility, with occasional visits to Government facilities, primarily in the Washington, D.C. metro area. All contractor personnel must be capable of being cleared to enter a DoD space per applicable DoD and Pentagon Force Protection Agency standards.

7.0 GOVERNMENT FURNISHED EQUIPMENT (GFE), PROPERTY (GFP), MATERIALS (GFM):

☒ **None;** the vendor will procure or provide all necessary components of a development environment using a commercial cloud vendor (virtual machines, databases, etc.), all necessary equipment to access the development environment (computers, network hardware), and any software licenses needed for development.

8.0 SYSTEM ACCESS

The vendor will require access to unclassified U.S. Government and other commercial systems used to collect background information on Subjects during all parts of the process. This access will include service providers' Test and Production environments, and covers both the submission of new queries and reading/retrieving/storing their results. The vendor must adhere to all security and privacy requirements imposed on any entity with access to Government-furnished information.

9.0 TECHNICAL CONTACT

Patrick Stoddart
Defense Digital Service
patrick@dds.mil
415-506-7294

10.0 AGREEMENTS OFFICER

Khalil Mack
Washington Headquarters Service - Acquisitions Directorate
khalil.r.mack.civ@mail.mil
703-545-9507

11.0 MILESTONES

Funding will be released to the vendor following each satisfactory delivery of two iterations, or approximately monthly.

Payments for this activity will be Firm Fixed Price per iteration. The Government is paying for the repeatable process resulting in the delivery of functional products which meet the definition of done established at the start of each iteration. At a minimum, the definition of done will include: functioning product/code, user acceptance testing, and automated security testing. See section 4.2 for additional technical requirements.