Providing Reliable Assistance Faster: Secure, Modern, Mission-Capable Credentialing to Support Disaster Operations

Deena Disraelly
Institute for Defence Analysis
Virginia USA

Laura Itle
Institute for Defence Analysis
Viriginia, USA

ABSTRACT

The public sector, including state and local government, public health, and emergency management; the private sector; and the Federal Government jointly face challenges with rapidly collecting and validating credentials for individuals applying for employment or volunteering for emergencies, vetting security clearances, and ascertaining suitability. In 2017, for instance, credentialing gaps delayed employees and volunteers from contributing much-needed skills in disaster areas during one of the worst hurricane and wildfire seasons on record while Federal agencies inadvertently issued interim clearances to individuals with criminal records. We propose a secure, modern, mission-capable information technology solution to these with the United States Postal Service hosting this streamlined process by serving as the hub for collection, validation, and transfer of pertinent data. The solution would introduce access points in over 5,000 communities for citizens participating in disaster support operations, as well as those requiring credentialing for employment as part of day-to-day operations.

Keywords

Credentialing, Disaster Support, Clearance, Suitability, Volunteer.

INTRODUCTION

In 2017, a backlog of more than 300,000 initial clearance investigations resulted in Federal agencies inadvertently issuing interim clearances to individuals with criminal records. In that same year, credentialing gaps prevented employees and volunteers from serving in disaster affected areas from one of the worst hurricane and wildfire seasons on record. In 2018 and 2019, a state National Guard assumed responsibility for reconstruction of several hundred homes following flooding damage; they found themselves faced with hundreds of potential crews available to support construction efforts immediately but whom they could not immediately employ while they waited on credentials and background checks.

There is, within the Federal government and across the public and private sectors, a current inability to adequately vet credentials for emergencies, unnecessary redundancy which increases government costs and wastes citizen time, and avoidable mistakes in issuing clearances. While efforts have been made to create centralized repositories of volunteers both for specific roles (e.g., medical volunteers assisting in disasters) and more generalized interest as exists in volunteer-matching initiatives, most volunteer registration and nearly all volunteer credentialing remains decentralized to individual organizations or units within organizations.

This paper describes a concept to address these credentialing, suitability, and clearance (CSC) challenges and help put people to work faster both in supporting disaster operations and as part of their day-to-day jobs. The proposal was developed for the Federal Government's Government Effectiveness Advanced Research (GEAR) Center Challenge in coordination with a range of government and public sector stakeholders and has not yet been implemented.

OBJECTIVE

We propose the development of a secure, modern, mission-capable information technology (IT) solution hosted by the U.S. Postal Service (USPS) to support data collection, validation, and transfer and to streamline the modern clearance, suitability, and credentialing process. This effort introduces access points in over 5,000 communities for citizens requiring background checks and other digital identification and supports the Post Master General's Digital Initiatives. The effort harnesses a multi-sector public-private partnership to rapidly prototype new strategies and models for digital identification as well as lay the groundwork for continued innovation of Government operations and services based on private sector and academic research and best practices. Further, this effort aims to include a State-based pilot study integrating existing fingerprinting capabilities with electronic document validation and background checks and creating personal digital identity records for use by the whole of the Federal government and State, local, tribal, and territorial (SLTT) and private sector partners—to perform credentialing, suitability, and clearance adjudications.

APPROACH

Our solution links individuals and organizations to identity proofing and subsequent activities required for CSC. Our solution includes two principal use cases that will be useful to the Federal Government and a variety of other end users: (1) day-to-day operations and (2) disaster support operations. These are illustrated in Figure 1 and described below. The numbers in parentheses in the text correspond to each step of the illustrated process.

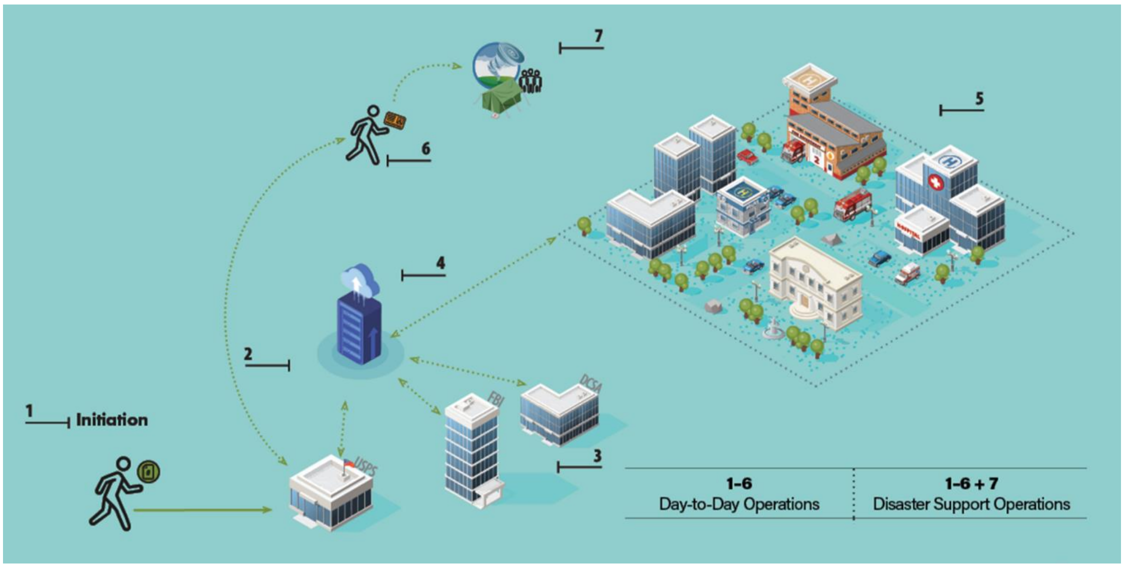

Figure 1. Detailed Solution for Day-to-Day Operations and Disaster Support Operations

Day-to-day operations (D2D)

The D2D use case is used for scenarios that require routine identity proofing and verification—background checks for employment, volunteering, and adoption; document validation to meet employment, volunteering, or insurance requirements; and biometrics to initiate clearance, suitability, and some credentialing investigations, to name a few. For example, a typical D2D process starts when a Federal agency sends a new hire a QR code to initiate a clearance, suitability or credentialing investigation. The new hire takes that code to any local USPS post office—(1) initiation. A USPS clerk who is vetted with a tier 1 background check verifies the new hire's identity in-person by checking approved Federal or State identification (ID), passport, or military ID—(2) identity proofing. The USPS clerk scans and electronically mark as validated (having been) provided by a known individual—any documents requested by the hiring agency (such as copies of diplomas and transcripts, Social Security card, military discharge documents, certifications, and other credentials)—(2) document validation. The USPS clerk also scans the new hire's fingerprints on the Live Scan (or similar) device and submits the fingerprints—(2) check initiation—to the cloud for the Federal Bureau of Investigation (FBI) or the Defense Counterintelligence and Security Agency (DCSA). The FBI or DCSA retrieve the fingerprints, conduct the background or identity history summary check (BC or IdHSC), and conduct any additional required investigation—(3) background check/investigation. The collected data and completed background check and investigation are sent to a cloud address specified by the QR code—(4) CSC data transfer—from which the hiring organization retrieves it—(5) CSC data retrieval. The USPS clerk may provide the new hire with a digitized data card with copies of all of the information collected during the encounter or have the card delivered once more detailed background checks are complete—(6) CSC data card creation.

This same process could be employed by, for example, schools hiring new teachers; hospitals hiring new medical professionals; and nonprofits and nongovernmental organizations (NGOs) recruiting volunteers to work in disaster zones or with children, seniors, or animals. A simplified process—one that only identity proofing and background checks—could be used by companies that maintain a bonded workforce for insurance purposes (e.g., moving and repair companies). Identity proofing for passport issuance is already in place at USPS locations and could be further expanded to include remote, in-person proofing to obtain digital identification certifications for government websites and online applications. The receiving organization will identify the appropriate type of check as a function of the role of the individual being credentialed.

Security for personal data is of paramount importance, especially during data transfer to credentialing organizations and then from credentialing organizations to recipient hiring/volunteer organizations. As envisioned, the hub organization collecting materials will not store materials and will serve only as a pass-through. Materials in transit will be encrypted and sent to specific encoded addresses generated as part of the credentialing initiation.

Disaster support operations (DS)

The DS use case is for scenarios that require rapid, accurate credentialing to put volunteers and professionals in place to provide support during disasters (e.g., volunteers in shelters and registration centers and medical and hazardous materials professionals serving affected populations). For example, if the D2D concept hiring organization is a voluntary organization active in disaster (VOAD) member, it now has the credentials for volunteers it is deploying to do home inspections, repairs, and rebuilding, including the new hire. The new hire brings the CSC data card to the Incident Command Admin Section on arrival. A USPS clerk working as part of the Admin Section uses the card to rapidly register the hire and validate his/her credentials— (7) rapid credential check.

In advance of the deployment, the VOAD organization could also provide the local USPS with a list of volunteers and obtain a validated copy of all the credentials and IdHSC results for the team. The team leader could provide this onsite to the Admin Section Chief to rapidly authorize the team to begin providing needed services citizens in the impacted area. In both cases, the volunteers will be out assisting the community as quickly as possible, and the Admin Section will have a clear record of its volunteers and their credentials for ease of accountability. The year-one pilot will culminate with a demonstration of this capability conducted as part of a State- or local-run exercise.

REAL-WORLD APPLICATION

Following a series of state-wide challenges, in 2019, a state National Guard assumed responsibility for directing reconstruction, replacement, and repair of more than 400 homes damaged in flooding. The National Guard found themselves facing the recruitment, hiring, and assignment of crews that would conduct the reconstruction efforts in homes across the state. In addition, National Guard members, many of whom had security clearances or background checks to perform their Guard functions, also required credentialing to support specific roles if they were participating in the reconstruction efforts through their civilian jobs. When facing the same scenario in the future, if the proposed CSC capability existed, crews could complete background checks and validate credentials prior to arriving at reconstructions and repair sites. Each crew member would carry an identification card with the checks and credentials. Therefore, when they check in at their sites or at a centralized assignment hub, the cards could be read and all of their pertinent information to support site work and specialized skills would be available for immediate reference. They would be more rapidly, effectively, and safely assignable.

In addition to the recovery efforts, members of the National Guard are also actively involved in reducing drug demand in the state's school system. These members provide mentoring and engagement to teach youth leadership, civic duty, self-esteem, and drug awareness. Right now, they go through an additional background check to volunteer in schools. In the future, a strategic partnership with state agencies, schools, and communities could be developed such that previously cleared and credentialed National Guard members would be able to access their own records. Likewise, the state's National Guard could provide access to those records so that local school systems could check the current status of volunteer members. This would result in a reduced cost and time for background checks and enable volunteers to engage with young people sooner and more effectively.

The state's National Guard has already expressed interest in this or a similar solution noting that emergency managers and state and local politicians are going to want to ensure that everyone working the crisis or working with children is certified.

CONCLUSION

The proposed solution responds to several recent government calls to action regarding CSC. In March 2018, the President's Management Agenda recognized the need to address CSC issues, and in May 2019, the Government Accountability Office recommended that government agencies adopt more secure identity proofing practices after finding that use of personally identifiable information (PII) questions for online identity proofing were subject to data theft–related fraud.

Building a solution to these challenges requires both resources and Federal coordination among agencies with responsibilities for CSC, as well as buy-in from State, local, tribal, and territorial government(s); nongovernment organizations; and individual volunteers. However, the benefits of a central, accessible means to rapidly credential and grant access to employees in day-to-day operations would increase efficiency and reduce government and employer costs. In response to a crisis, the solution represents a rapid method to verify the identity of responders and volunteers and validate their expertise, allowing faster deployment of human assets in the way that will provide the most impact to affected communities. Changing current processes may not be easy, but providing reliable assistance to impacted citizens is worth the challenges, particularly, as shown above, a technical solution is possible.

ACKNOWLEDGMENTS

We thank Laura Odell, Steve Olechnowitz, John Adams, Michael Lippitz, Michael Dominguez, David Nicholls, Patricia Sadiq, Matthew Coursey, and Linda Garlet for their ideas and support throughout this process and thank our corporate headquarters for their support of this proposal. We'd also like to thank the partner organizations who contributed to our GEAR Center Challenge concept. Lastly, we thank the U.S. General Services Administration and the Office of Management and Budget for recognizing this proposal with an Honorable Mention in the GEAR Center Challenge.