Vets.gov Saving In Progress Forms Risk Based Assessment
Date: July 28, 2017
Subject: Saving in Progress Forms at AAL1

Background:
This memorandum describes the reasoning for allowing Vets.gov users with only a username and password to save in progress forms and come back later to complete or submit the form. To save a form, a user must be logged in to Vets.gov; the question at hand is what authentication method should be required for this functionality.

The way Vets.gov stores saved information is no different based on how a user logged in; in all cases, all user-entered information is encrypted while stored and only accessible by re-logging in with the user's credentials.

SP 800-63-3 Concepts and Definitions
In NIST SP 800-63-2, the concept of Level of Assurance (LOA) existed, but in SP 800-63-3, which was released in June 2017, this concept has been split out into Identity Assurance Level (IAL) and Authenticator Assurance Level (AAL). Following the guidelines in SP 800-63-3, "the selection of IAL can be short circuited to IAL1 if the agency can deliver the digital service with self-asserted attributes only." Given that no attributes need to be validated for saving, nor later re-populating or submitting these forms on Vets.gov, IAL1 is appropriate for this functionality and identity proofing is not required.

According to NIST SP 800-63-3, the appropriate AAL when showing personal information, including self-reported personal information, to the user is AAL2, which requires multi-factor authentication (MFA). This is supported by the following quotes from the document: "MFA is required when any personal information is made available online" and "Release of even self-asserted personal information requires account protection via MFA. Even though self-asserted information can be falsified, most users will provide accurate information to benefit from the digital service. As such, self-asserted data must be protected appropriately."

In SP 800-63-3, Section 6, multiple "impact categories" are identified. The two risks relevant to this situation are "unauthorized release of sensitive information" and "harm to agency programs or public interests." This risk of having AAL1 (no MFA) for saving forms is that if a user's account credentials (username and password) are compromised, that user's saved information could be exposed to a third-party. If this "unauthorized release of sensitive information" were to occur, it could harm not only that individual, but also the VA's reputation as a whole. Given that those two risks exist, SP 800-63-3's guidelines say AAL2 should be used when "making person data accessible," even if these risks are "low" or "moderate."

Factors in the Decision:
Given that SP 800-63-3 states showing personal information should require AAL2, to allow Vets.gov users to save forms at AAL1, Vets.gov needs to make and

document this risk-based decision. Two driving factors for this risk-based decision are:

1) Those applying for benefits on Vets.gov, such as health care, pension, and (later in 2017) disability compensation benefits, are often in difficult or vulnerable situations. This includes both homeless Veterans, who may not have a landline or cell phone needed to successfully complete multi-factor authentication, and older Veterans, who may not understand how to set up and use multi-factor authentication.
2) Additionally, some of these forms are expected to take over an hour to complete, with data needed to be compiled and entered from multiple sources; it is not reasonable to force users to complete these forms in one sitting.

The combination of the above two bullets means that to balance protecting user privacy with allowing all users to be able to complete these forms successfully and with a reasonable user experience, Vets.gov should take on the risk of not requiring multi-factor authentication when saving a form in-progress.

Vets.gov should promote users enabling MFA on their accounts through both marketing and training, but it should not be required if users are unable to set up MFA. Additionally, if users are logged in without multi-factor authentication, Vets.gov should provide content that clearly articulates the risk of saving any personal information, so that the user can make an informed decision about whether they want to save the form or complete and submit it in a single sitting. For this reason, Vets.gov should not automatically save any information for an AAL1 user, letting the user make the decision if they want their information stored.

Privacy Office Opinion
The current, most widely used VA site for completing online forms, eBenefits, allows users to save forms without two factor authentication. From the VA Privacy Office perspective, therefore, there is precedent for allowing this functionality with only a username and password, this functionality has already been approved and in use at VA for many years, and this memo supports the existing precedent.

Decision:
Saving a form in progress is an expected feature of websites today and something that should not be limited to users who can successfully add multi-factor authentication to their accounts. We acknowledge there is a risk in this decision; for Vets.gov's audience and functionality, the additional user experience benefit of allowing AAL1 users to save forms outweighs the risk for user-entered information to be viewed if individual account credentials are compromised.

Signed Charles Worthington 1510392

Digitally signed by Charles Worthington 1510392
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=charles.worthington@va.gov, cn=Charles Worthington 1510392
Date: 2017.07.31 09:49:34 -04'00'

Charles Worthington, VA CTO

Signed CLARE MARTORANA

Digitally signed by CLARE MARTORANA
DN: c=US, o=U.S. Government, ou=Executive Office of the President, cn=CLARE MARTORANA, 0.9.2342.19200300.100.1.1=11001003443013
Date: 2017.07.31 11:26:07 -04'00'

Clare Martorana, Vets.gov lead

Signed Griselda Gallegos 204736

Digitally signed by Griselda Gallegos 204736
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=griselda.gallegos@va.gov, cn=Griselda Gallegos 204736
Date: 2017.08.02 11:50:45 -05'00'

Griselda Gallegos, Vets.gov ISO

Signed Angela Gant-Curtis 105447

Digitally signed by Angela Gant-Curtis 105447
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=angela.gant-curtis@va.gov, cn=Angela Gant-Curtis 105447
Date: 2017.07.31 10:31:58 -05'00'

Angela Gant-Curtis, Vets.gov System Owner

Signed RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=rita.grewal@va.gov, cn=RITA K GREWAL 114938
Date: 2017.08.02 09:45:51 -04'00'

Rita Grewal, Vets.gov Privacy Officer