# GI Bill Data Service 2FA Mandate Proposal

10/8/2017

Patrick Vinograd – Ad Hoc LLC – Vets.gov DevOps Lead

## Executive Summary

In order to satisfy the CIO 2FA mandate, we propose to use ID.me as the sign-in and two-factor authentication mechanism for the GI Bill Data Service (GIDS), a supporting administrative application of Vets.gov.

## Background

* The GI Bill Data Service is an administrative application used to aggregate data about educational institutions. The aggregated data feeds the GI Bill Comparison Tool feature of Vets.gov.
* The user base of GIDS consists of VA employees and (currently) one non-VA subject matter expert.
* GIDS is deployed along with the rest of the Vets.gov infrastructure in AWS GovCloud. It currently uses single-factor (username/password) authentication.

## Challenge

The default mechanism for satisfying the 2FA mandate is to use PIV authentication via SSOi or SSOe. Neither of these options appears to be appropriate for GIDS.

* Because one key user is neither a VA contractor nor employee, he is unable to access the VA network via VPN and therefore cannot access SSOi.
* The IAM team has determined that SSOe is not an architecturally appropriate choice for GIDS given that it is an internal-facing application with a small user base.

## Proposal

Instead of using PIV-based login, we propose use ID.me two-factor authentication to enable access to GIDS.

Vets.gov as a whole is already closely integrated with ID.me as its primary identity provider/broker. We can extend this integration to GIDS, and enforce a condition that authorized users must be enrolled in two-factor authentication (which is currently optional for general access to Vets.gov).

GIDS will continue to maintain a list of authorized users; once a user has signed in with ID.me, GIDS will ensure that the user has permission to access the application.

The application architecture of GIDS differs from the rest of Vets.gov, so rather than add GIDS as a second SAML service provider, we intend to use a “re-authentication” pattern using Vets.gov API tokens. This approach is described in more detail at the end of this document.

## Rationale

* ID.me is already an accepted technology within VA. It is used to control access to user’s PII and PHI data for Vets.gov. It is also now an approved sign-in partner for SSOe (via access.va.gov).
* By re-using our integration with ID.me, Vets.gov maintains a single identity provider rather than incurring the operational overhead of also integrating with SSOi or SSOe to serve a small number of users.
* The data managed by GIDS consists of publicly available, general information about colleges and companies related to GI Bill benefits. It contains no PII or PHI. Accessing GIDS should not require the extremely high level of assurance (LOA4) provided by PIV issuance.
* In this context, the key security assurance to enforce is adequate control of credentials, which is satisfied by requiring two-factor authentication. The identity of GIDS users is sufficiently assured by the fact that nobody is given access to GIDS without being personally known to the GIDS business owner (e.g. by being a member of her organization). This organizational assurance trumps any programmatic assurance that would be gained by enforcing LOA3 login/identity-proofing. For that reason we intend to require LOA1 login with multifactor authentication.

## Implementation Notes

This section describes in detail how GIDS will leverage the existing Vets.gov authentication and API token mechanism.

1. Users will be required to first access [www.vets.gov](http://www.vets.gov) and sign in using the existing ID.me login mechanism.
2. The user’s browser session will now contain a valid vets.gov API token.
3. Users will then visit the GIDS application at [www.vets.gov/gids](http://www.vets.gov/gids) and click a button to access GIDS.
4. Since this application is hosted as a sub-page within vets.gov, the vets.gov API token continues to be available. The browser will make a request to GIDS, supplying the API token.
5. GIDS will forward this request to api.vets.gov, requesting the user profile for the supplied API token.
6. If the token is invalid or expired, api.vets.gov will deny access, and GIDS will likewise deny access.
7. If the token is valid, GIDS will examine the supplied user profile. The user profile contains the user’s identity (in this case email address), and a flag indicating whether they logged in with two-factor authentication.
8. If two-factor authentication was not used, or if the given identity is not an authorized GIDS user, GIDS will deny access.
9. If instead the user is authorized and has used two-factor authentication, GIDS will establish a standard authorized browser session and the user can proceed to use the GIDs application features.

Per the above, we approve the use of ID.me two-factor authentication to control access to the GI Bill Data Service application.

<signatures>