October 7, 2024

National Institute for Standards and Technology
100 Bureau Drive (Mail Stop 8940)
Gaithersburg, Maryland 20899-2000

Re: Digital Identity Guidelines - Revision 4 - 2nd Public Draft

To: David Temoshok et al

The Digital Benefits Network at the Beeck Center for Social Impact + Innovation at Georgetown University, respectfully submits this comment in response to the National Institute for Standards and Technology's (NIST) call for comments on their second public draft of version four of the Digital Identity Guidelines (Special Publication 800-63). The Digital Benefits Network supports government in delivering public benefits services and technology that are accessible, effective, and equitable in order to ultimately increase economic opportunity. The Digital Benefits Network has been pursuing work on digital identity in public benefits since mid-2022, and in May of this year entered into a Collaborative Research and Development Agreement with NIST and the Center for Democracy and Technology to adapt NIST's guidelines to benefits delivery contexts.

We appreciate that in these updated guidelines, NIST has explicitly incorporated equity and accessibility throughout the guidance. We believe this is particularly important for these guidelines to be useful to public benefits administering agencies who must balance access, security, and accuracy.

Comments on Base Volume

Section 3: Digital Identity Risk Management (DIRM)

We are pleased to see that the updated guidelines introduce the step of "Defining the Online Service." We believe this will be a valuable step for public benefits administering agencies evaluating risk that can be mitigated by and/or caused by identity systems.

In introducing the DIRM process, NIST notes a requirement (lines 1062-1064) for consultation with "a representative sample of the online service's user population to inform the design and performance evaluation of the identity management approach."

We believe it may be helpful for NIST, in the guidelines or in supplemental materials, to provide agencies with examples of what meaningful consultation looks like as part of a DIRM process. This could also involve making reference to existing federal resources, (e.g., U.S. EPA: Capacity Building Through Effective Meaningful Engagement; User Experience – Digital.gov, User Research and the Paperwork Reduction Act | United States Digital Service) and other outside sources.

Section 3.5.6 Continuously Evaluate and Improve, Performance Metrics
We are also pleased to see that the DIRM process emphasizes the importance of continuous improvement and evaluation, and appreciate that the guidelines offer examples of performance metrics that agencies should consider.

Given the salience of discussions of fraud and waste in public benefits programs, we also believe that the metrics should emphasize the need to evaluate how often digital transactions that are suspected of being fraudulent are ultimately confirmed as fraudulent. This would encourage and help agencies to evaluate if their fraud detection approaches may be creating undue friction in comparison to outcomes. This measurement is in some ways implied in current metrics but could be made more explicit. It may also be valuable to include a metric focused on the number of account recovery attempts that are *successful*.

Section 3.6: Redress
We appreciate that NIST has addressed the importance of redress related to identity management processes. In particular, we are pleased to see the emphasis on making information about redress processes "documented, accessible, trackable, and usable by all people, and whose instructions are easy to find on a public-facing website" (lines 1765-1766).

We also appreciate that the draft emphasizes that "RPs and CSPs SHALL educate support personnel on issue handling procedures for the digital identity management system, the avenues for redress, and the alternatives available to gain access to services" (lines 1778-1780). Particularly in the context of public benefits delivery, staff responding to identity management issues may work for a contracted partner organization. While this may be beyond the scope of this draft, we believe NIST might consider providing guidance in the future about the types of education

that RPs and CSPs should provide, or that agencies should request in contracting language (e.g., that redress training must emphasize trauma-informed practice).

Section 3.7 Cybersecurity, Fraud, and Identity Program Integrity
We agree that identity management should not be considered in a vacuum, and appreciate that the draft emphasizes the need for "Close coordination of identity functions with teams that are responsible for cybersecurity, privacy, threat intelligence, fraud detection, and program integrity" (lines 1793-1795).

We believe this section of the guidelines is particularly important given the current benefits delivery context in which many state agencies contract with external vendors/partners to perform key identity management functions. We are aware that a current problem for state agencies is having access to information about how their implemented identity management approaches are working, and believe it is important for the guidelines to emphasize the need for privacy-preserving but reliable ways for RPs (e.g., state agencies) to understand performance of processes carried out by external CSPs.

Comments on Volume A:

Considering the primary context of the DBN's work, digital delivery of public benefits in the US, and the diverse populations served by these programs, with different needs and different technology access, we appreciate that the guidelines emphasize multiple methods and pathways for performing critical identity management functions, including identity proofing (e.g., lines 489-494). While not required for every benefits delivery scenario, we appreciate that the second public draft provides greater clarity on pathways for identity proofing at IAL2 to make non-biometric, digital evidence, and biometrics pathways clearly understandable.

Section 3.1.8: Requirements for Confirmation Codes
We appreciate that NIST is including validated physical addresses as an option for receiving confirmation codes (lines 1147-1148). We also appreciate that NIST is allowing for codes to potentially remain valid for up to 21 to 30 days when sent to validated domestic and international postal addresses respectively. Based on information gathered from advocates in states where physical address confirmation has been incorporated as an identity proofing step in public benefits delivery, when confirmation codes are only valid for a very short period of time (e.g., less than ten days), it may mean some individuals are unable to use codes successfully. Recognizing that this may not be appropriate for all cases, NIST may want to

consider recommending minimum time periods during which codes remain valid, to avoid blocking individuals from successfully completing identity proofing processes.

Respectfully,

The Digital Benefits Network, Beeck Center for Social Impact + Innovation at Georgetown University