PRELIMINARY SECURITY REQUIREMENTS REALITY TESTING
Clark ***D R A F T***

Thanks for agreeing to give us (IDESG and its Framework Management Office staff) time to discuss the feasibility of our plans for possible industry evaluation and feedback on the IDESG's draft Functional Requirements for Cybersecurity, and proposals for a self-attestation program.

The following requirements, drafted by the Security Committee, obviously are an early-stage, draft set which will be refined by stakeholder feedback and finalized (as a v1 set) in mid-2015. Questions for discussion follow the list of draft requirements.

Your input on both the requirements, and the proposed discussion questions, is solicited and very welcome. We're hoping to refine this inquiry for broader use, and further interviews with various parties. We will welcome all suggestions for improvements (as well as what kinds of stakeholders we ought to be querying).

We will honor nonattribution rules for this discussion, and pass along only anonymized, paraphrased feedback to the IDESG community ("Chatham House rules").

PRELIMINARY DRAFT OF FUNCTIONAL REQUIREMENTS (CYBERSECURITY ONLY)

[Abridged from Security Committee, 2015-01-15 version:
https://www.idecosystem.org/wiki/File:Security_Requirements_DRAFT_v._1.0_(20150115).xlsx.]

1. Service providers in the ecosystem follow recognized information security standards, frameworks, and/or appropriate practices.

2. Each account credential pair is uniquely identifiable for authentication purposes.

3. The confidentiality and integrity of identity data (e.g., attribute values) is protected during the execution of all identity functions and across the entirety of the data lifecycle (collection through destruction).

4. Credential and token issuance processes protect against unauthorized disclosure and/or reproduction.

5. Users are able to authenticate the source of all token and credential data received from service providers.

6. Credentials and associated tokens are granted to the appropriate and intended user(s) only.

7. There are clear processes, policies, and procedures in place for the execution of identity functions.

8. End users have access to the policies and procedures in place for the execution of identity functions.

9. The confidentiality and integrity of authentication data are protected. Data (such as passwords and passphrases) used for authentication are never stored in plaintext.

10. User control of the token is proven during the authentication process.

11. Users must be able to choose authentication mechanisms that are stronger than single factor passwords and passphrases and are commensurate with the level of risk associated with the transaction.

12. Service Providers have established policies, procedures, and processes in place to maintain availability of services.

13. Where cryptographic solutions are used, key management policies and practices are established and used consistent with industry standards and best practices.

14. Processes for the reissuance and/or recovery of credentials and authentication tokens are commensurate with the original process and procedures followed during registration and credentialing core operations, including identity assurance procedures.

15. Transactions and security events (to include the execution of identity functions) are logged in a manner that supports system audits and, where necessary, security investigations. Timestamp synchronization and granularity are appropriate to the level of risk associated with the environment, sector, or transaction.

DISCUSSION QUESTIONS

A. Who's covered by these? Who should be? Do the requirements sufficiently address the needs of multiple stakeholders in a given identity federation?

B. Where is the "authority"? Are there other sources of guidance or similar requirements that ought to be integrated into or mapped to these requirements, so that they're more meaningful to possible self-assessors?

C. When can criteria like these reasonably start to matter? Are these requirements or some subset generally appropriate as a "baseline" of entry-level requirements for self-attestation, feasible in 2015 for broad use? (As opposed to stretch goals, or operationally over-ambitious.)

D. What are useful requirements for self-*assessment*? Can a requirements set like this be useful to identity ecosystem stakeholders -- including IdPs, RPs and citizens -- as a basis for effective self-assessment? What additional information or elaboration would make them more relevant or adoptable?

E. How can requirements be incorprated into relevant ecosystems? What can IDESG reasonably offer, if anything -- an instrument, trust marking program, self-

assessment template, registry or resource -- to promote self-*attestation* of this kind, by stakeholders, on a more coordinated basis? Are there successful models to which we should look? How can we avoid the unattractive features of some prior standards certification programs? What can the IDESG do to add value? What can US policy and regulation do, potentially?