IDESG Standards Nomination Evaluation Checklist

Standard Name: This evaluation comprises three companion OAuth 2.0 framework standards and one informational OAuth 2.0 specification. (see 'Reviewer Comments')	RFC 6749, The OAuth 2.0 Authorization Framework (Standard) RFC 6750, The OAuth 2.0 Authorization Framework: Bearer Token Usage (Standard) RFC 7009, OAuth 2.0 Token Revocation (Standard) RFC 6819, OAuth 2.0 Threat Model and Security Considerations (Informational)	**Acronym**	OAuth 2.0
Submitter Name:	Sal D'Agostino	**Email:**	sal@idmachines.com

Consistency with NSTIC Guiding Principles		
Guiding Principles	*Is Consistent With*	*Comments*
Privacy Enhancing and Voluntary	☒	OAuth 2.0 is an authorization framework supporting the delegation of controlled access to protected data resources. It is intended to preclude the need for users to divulge passwords and other private information when requesting 3rd party services, solving the password anti-pattern problem.
Secure and Resilient	☒	Focused on three common client profiles (web application, user-agent-based application, and native application), RFC 6749 presents guidelines for addressing 16 security considerations. RFC 6819 provides additional important guidance for security considerations based on a defined threat model. Access management (token management) is an essential aspect of a secure and resilient identity solution. RFC 7009 extends RFC 6749 to support token management by enabling revocation of access and refresh tokens that are no longer needed, allowing the authorization server to clean up security credentials that are no longer in use.
Interoperable	☒	OAuth 2.0 prioritizes flexibility over interoperability. It provides many optional components for broad applicability, but does not specify conformance clauses which would enforce the development of 'web-scale' interoperable implementations. In providing a flexible framework, OAuth 2.0 puts interoperability into the hands of those implementing the standard to foster and develop an interoperable ecosystem. Together, the standards included in this evaluation provide the building blocks for interoperable solutions. OAuth 2.0 is an extensible authorization framework developed to address limitations in OAuth 1.0 (RFC 5849). OAuth 2.0 does not provide backward compatibility with OAuth 1.0.
Cost Effective and Easy to Use	☒	OAuth 2.0 provides a delegation and authorization framework that is, for the most part, invisible to an end-user. When implemented

		with a robust authentication scheme, it facilitates leveraging existing identity credentials across a variety of service providers, reducing the need for users to create, store, or remember a multitude of passwords and login credentials. This directly supports the IDESG goal to reduce cost of online transactions. The standard itself is free. It has been implemented, and is available and in use by many applications and services. This suggests that implementation is not burdensome for large enterprise providers, although channels suggest substantial implementation hurdles for smaller scale development efforts. Several open-source implementations are available to ease the implementation burden.
Decision Criteria (SAP Section 4)	**Meets**	**Comments**
Standards Developer		
Participatory openness (4.2)	☒	The IETF uses an open process. There is no formal membership and no dues. Since the IETF has no formal membership, decisions cannot be made by voting; they are made based on rough consensus. Work of the IETF is accomplished through Working Groups. Individuals join the mail lists of Working Group(s) in which they have interest and participate remotely through email and conference calls. Participants also may attend in-person WG meetings. Annual and interim in-person WG meetings are held internationally. Often a majority of the work and decision-making takes place at the in-person meetings, so depending on the location of the participant and of the meeting, potentially significant travel expenses could be incurred by those wishing to effectively participate in the WG activities. By participating, an individual automatically accept the IETF's rules.
Fairness and due process (4.2)	☒	Processes are administered by the Internet Engineering Steering Group (http://www.ietf.org/iesg/) which is directly responsible for the actions associated with entry into, and movement along, the Internet "standards track" including final approval of specifications as Internet Standards. Input and feedback on the process is made through discussion forums open to anyone. The process includes Review and Appeals. Any action made by an Area Director or the IESG may be made the subject of the conflict resolution mechanisms set out in Section 6.5 (Conflict Resolution and Appeals) of RFC 2026. Processes are well documented at http://www.ietf.org/about/standards-process.html and http://www.ietf.org/about/process-docs.html.
Transparency (4.2)	☒	Open IETF announcement and discussion mailing lists are central to IETF activities. Every WG has a dedicated mailing list. These mail lists are viewable by anyone through http://datatracker.ietf.org/wg/ and anyone can post to them, although posting by non-members is subject to review by the moderator. To maintain the transparency of the Working Group process, IETF

		imposes rules for advance notice on time and place of Working Group meetings. Schedules and agendas are available in advance on the IETF web site. It is up to participants to keep abreast of postings relevant to the activities they are involved in. Information on RFCs and on active and concluded Working Groups can be found on http://datatracker.ietf.org/.
Adequate public review process (4.3)	☒	During the development of a specification, major draft versions of the document may be made available for informal review and comment by placing them in the IETF's Internet-Drafts directory. Review guidelines are published at http://trac.tools.ietf.org/area/gen/trac/wiki. The IETF standards lifecycle is described in Section 6 of RFC 2026 *The Internet Standards Process Current Best Practices* as updated by RFC 6410 *Reducing the Standards Track to Two Maturity Levels*.
Stable hosting arrangements (4.3)	☒	The IETF standards process artifacts are hosted and archived on http://www.ietf.org/. IETF discussion lists are archived for anonymous HTTP or FTP access at ftp://ftp.ietf.org/ietf-mail-archive or in a web-based archive. Requests may be made to a list's "-request" address.
Sufficient intellectual property rules (4.3)	☒	The IETF intellectual property rights rules are defined in RFC 3979, "Intellectual Property Rights in IETF Technology." Contributors must make IPR disclosures which are viewable at https://datatracker.ietf.org/ipr/. The primary objective of this IPR policy is to obtain from the document authors only the non-exclusive rights that are needed to develop and publish IETF Documents and to copy, implement, and otherwise use IETF Contributions in the IETF Standards Process and elsewhere. IETF rules include some requirements for disclosure of patent claims, and include a routine request to claimants for RAND licensing, but appear not to seek, nor impose a requirement of, royalty-free licensing. The IPR license declarations against OAuth can be seen here: https://datatracker.ietf.org/ipr/search/?draft=&rfc=6749&submit=rfc&doctitle=&group=&holder=&iprtitle=&patent= By participating, an individual automatically accepts IETF rules about intellectual property (patents, copyrights and trademarks). If working for a company, and working within the IETF is part of the job, a person must obtain clearance from their company (although the IETF views participants as individuals and never as a company representatives).
Nominated Standard		
Relevance to IE (4.2)	☒	See 'Guiding Principles' above. In support of the IE, OAuth 2.0 delivers delegated access (authorization) to confidential resources providing a building block for IE solutions. While OAuth 2.0 is not itself an authentication protocol, authentication protocols can be layered to provide robust, secure, integrated authentication and authorization solutions.
Function-oriented description (4.2)	☒	OAuth 2.0 was designed to be open and flexible – no product-specific design features were specified. Requirements are

		abstracted through three common client profiles (web application, user-agent-based application, and native application) covering multiple potential uses cases and deployment scenarios. RFC 6750 describes how to use bearer tokens in HTTP requests, supporting a standardized mechanism for access to protected resources.
Affordability (4.2)	☒	The IETF has no membership fee. IETF standards are freely available and can be found at http://www.ietf.org/rfc.html. Three week-long in-person meetings are held each year at various international locations and are open to anyone. In-person attendees pay a registration fee but remote participation is free.

Recommendation to SCC					
Reviewer	**Anne Hendry**	*Accept*		*More Info Needed*	*Reject*
Reviewer Comments To satisfy the IDESG vision and realize the full value of the OAuth 2.0 Authorization Framework across a broad spectrum of uses and providers requires the three related standards: - RFC 6749 (OAuth 2.0 Authorization Framework), - RFC 6750 (OAuth 2.0 Authorization Framework: Bearer Token Usage) and - RFC 7009 (OAuth 2.0 Token Revocation). Additionally, the Informational RFC 6819 (OAuth 2.0 Threat Model and Security Considerations) defines a comprehensive threat model and provides important guidelines and countermeasures for thwarting threats that may be encountered in OAuth 2.0 implementations, so is included in this evaluation.			☒	☐	☐