Poster: Publishing Sensitive Cybersecurity Research

Dr. Deb Frincke, Brad Martin
ODNI/National Security Agency
Fort Meade, Maryland, USA

Amy Oaks LoPresti, Peter Dinsmore
The Johns Hopkins University
Applied Physics Laboratory
Laurel, Maryland, USA
Amy.Oaks@jhuapl.edu
Peter.Dinsmore@jhuapl.edu

***Abstract*—Dissemination, review, and reuse of ideas enable the advance of science, as well as recognition of individual contributors. Peer-reviewed journals have been created to meet the need of academia and government to publish scientific results. However, some government research, particularly in the area of cyber security, is considered sensitive, and therefore is barred from public release. Even though the community of researchers doing sensitive work has the same needs as those doing unrestricted research, the absence of a peer-reviewed publication process impedes the quality and progression of sensitive science relative to its public counterpart. To address this need, the Special Cyber Operations Research and Engineering (SCORE) Committee has tasked the Research Directorate of the National Security Agency (NSA) to establish a peer-reviewed journal for citable, sensitive (Controlled Unclassified Information [CUI] or classified information) cybersecurity research for the U.S. government and its affiliates.**

The NSA, aided by the Johns Hopkins University Applied Physics Laboratory (JHU/APL), undertook a project in November 2011 to determine the best venue for publishing sensitive cybersecurity research and pursued the following approach to creating a collaborative journal and publication process:

- Verify that no existing publication venue—governmental and nongovernmental societies, publishers, associations—publishes sensitive cybersecurity research.
- Determine candidate venues that either publish sensitive but noncyber research (*Journal of the Intelligence Community Research and Development*, *The Next Wave*), or cyber but nonsensitive research (*IEEE Security* and *Privacy*), and contact them for information.
- Survey potential subscribers, authors, and authoring organizations to gather requirements and interest in having a sensitive cybersecurity publication.
- Gather possible restrictions and impediments to publication, including classification, equities, release processes, and distribution techniques.
- Define a publication process flow that includes technical reviews, releasability review, and equities review, both within authors' originating organizations and between the originators and the nascent journal editors and publisher.
- Contact and nominate a candidate editorial board, drawing respected names from the computer and information security field, both in academia and government.

This effort has led to the creation of the *Journal of Sensitive Cyber Security Research* (JSCSR), which will be published in an online format available initially on the Intelligence Community's INTELINK (classified) website and soon after on the INTELINK-U (unclassified) site. It will feature an editorial board consisting of cyber luminaries from inside and outside of government, will utilize qualified peer reviewers, will solicit papers and results from around the U.S. cyber research community, and will produce quality publications using the paper-by-paper, publish to website model. The new journal addresses key challenges, presented in Table I, that have previously inhibited the creation and publication of a sensitive cybersecurity journal.

JSCSR realizes the SCORE committee's ideals, and will enable the safe dissemination of peer-reviewed, high-quality cybersecurity research with sensitivities ranging from CUI to Top Secret/Sensitive Compartmented Information (TS//SCI) to the rest of the intelligence community, government, contractors, and academic community with appropriate access in order to advance fundamental cybersecurity ideas in sensitive topic areas. The journal will stand up in calendar year (CY) 2012, with the initial call for papers expected this summer.

TABLE I. CHALLENGES AND SOLUTIONS

Challenge	JSCSR Solution
Information sharing hardships among potential collaborating research communities in government and academia that have appropriate authorizations and "need-to-know."	Provide information appropriately marked for classification and handling caveats initially at a widely-accessible TS/SCI site. In addition, the Journal anticipates implementing in CY 2013 repositories at the CUI and the Secret level.
Stovepiped processes and information that isolates results from other organizations.	The journal by its very nature enables a bridging of these stovepipes, providing a common repository for research results.
Lack of central mandate for establishing a collaborative journal.	By being sponsored by the SCORE Interagency Working Group, the journal has this mandate.