# Transition From Practice: A Proposed National Cybersecurity R&D Thrust

Sam Weber

Software Engineering Institute[1]

Carnegie Mellon University

samweber@cert.org

In addition to the existing NITRD strategy thrust emphasizing Transition To Practice (TTP), we would like to propose that NITRD prioritize "Transition **From** Practice": the engagement of researchers into operational activities, in order to foster research based upon operational needs.

The "Valley of Death" between research and commercialization is often bemoaned: although the Federal government spends more than $1 billion annually on unclassified cybersecurity research, it is sadly the case that too little of that work is commercialized. The current federal emphasis on Transition To Practice has done much to bridge this valley by helping researchers commercialize their results, but we believe that further assistance is necessary. In particular, we believe that bridge construction is more effective if one builds from both banks: we need to help researchers learn about operational and commercial needs and constraints so that they can plan their research accordingly.

 [2]

[1] Affiliation given for identification purposes only. The opinions stated in this document are those of the author, and do not necessarily reflect the official positions of the Software Engineering Institute or Carnegie-Mellon University.

[2] Image © State of New South Wales through the State Records Authority of NSW. Use authorized by http://www.records.nsw.gov.au/about-us/copyright-policy

Despite the talents and the best of intentions of academics, the cyber-attacks faced by various government agencies differ from those faced by universities, and few professors are familiar with governmental and commercial acquisition policies and regulations. For these and similar reasons, important operational issues can fail to attract research attention, and research results all too often do not correctly anticipate operational challenges. Bessey et. al's paper "A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World"[3] describes many such challenges that the authors encountered while commercializing their research tool. For example, they describe "the widely believed myth that programming languages exist": they found that significant markets are "awash" with non-standard and non-conforming compilers. Their original business plans hadn't even considered parsing customers' code as an issue, and instead they found that parsing real code was a very difficult problem.

We propose that federal agencies enable and encourage researchers to "embed" themselves in operational settings, such as working in DoD incidence response teams, or participating in security-sensitive software development teams, and then use these experiences to not only direct their research activities but also to inform the larger cybersecurity research community of operational challenges and opportunities.

Although internships and sabbaticals would, at first glance, appear to satisfy this need, in reality they almost always fail to do so. Because these activities are viewed as jobs and funded as such by the hosting organization, internships and sabbatical projects are usually carefully scoped so as to require little training – it isn't financially sensible to spend time and money training someone who will only be with the organization for a limited time – and this greatly limits the visibility of the researcher into the organization's activities. Furthermore, from a professor's point of view, engaging in operational activities is risky, as not only is it unpredictable what will be discovered, but the cybersecurity community, unlike the software engineering community, does not traditionally publish "experience reports".

Ideally, a Transition From Practice program could help incentivize operational embedding by researchers by helping offset a hosting organization's training costs and providing support for post-embedding research activities. As well, clearances and non-disclosure agreements are a traditional barrier and assistance in negotiating such would be beneficial. It is our belief that establishing such programs would not only help researchers cross the Valley of Death, but also make traditional TTP programs even more effective.

[3] Bessey et al., "A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World", CACM Vol.52, No. 2, http://cacm.acm.org/magazines/2010/2/69354-a-few-billion-lines-of-code-later/fulltext