RFI Response: Federal Cybersecurity R&D Strategic Plan

I. INTRODUCTION

Business Executives for National Security (BENS) is a nonpartisan, non-profit organization composed of over 440 senior executive members nationwide. Since its establishment in 1982, BENS has assisted government partners in developing best business practice solutions to our nation's greatest national security challenges. BENS is member-driven and financed, and does not accept government funding. Members participate in and fund the work BENS undertakes in their individual capacities.

The BENS Cyber & Tech Council (C&TC), formally launched in 2015, is engaged in several efforts related to technology policy, innovation, and cybersecurity. C&TC members recognize the importance of national-level planning in all aspects of cybersecurity and welcome the opportunity to contribute views. We commend the National Science and Technology Council (NSTC), the Networking and Information Technology R&D (NITRD) Program, and other relevant entities for soliciting comments on this critically important topic. BENS is available for additional consultations in this area and others at the intersection of business and national security.

II. SCOPE

In this comment, BENS seeks to identify several key cybersecurity-related issues that would benefit from increased emphasis—including through R&D—in government, industry, and academia. We note that, while a comprehensive and coherent R&D strategy for cybersecurity is of critical importance, cybersecurity-related education and training, adoption of best practices, and prioritization by leadership has the greatest potential to improve security over the near-term.

This comment is not intended to be comprehensive or exclusive of other areas. Indeed, we view the support of R&D in a diverse portfolio of emerging technologies as a sound investment strategy.

III. PERSISTENT PROBLEMS

In response to question #1 of the RFI, BENS would welcome additional R&D geared toward:

- **Increasing supply chain security**. Insufficient means exist at present to verify information and communications technology (ICT) component and system security, particularly at the physical or hardware layer. At present, organizations in the public and private sectors make significant assumptions of trust and conduct limited testing, often in an uneven and ad hoc manner. With recognition that supply chain management policies and practices are a key aspect of the solution, new technologies to test equipment with unclear provenance would fill a major security gap.

- **Strengthening data security.** Despite recent advancements in security technologies, many compromises still result in the exfiltration of significant quantities of sensitive data. In light of this, technologies that (a) aid in accounting for the whereabouts and usage of data; (b) impose additional authentication requirements on data when accessed, moved, or altered under unusual or unanticipated conditions; or (c) render data inaccessible or unusable outside of proscribed conditions or environments have the potential to improve data security. Concerted research toward these ends should merit a high priority.
- **Constraining the effects of vulnerabilities.** Recently-identified vulnerabilities in widely-used protocols, software, and software libraries has refocused attention on the security implications of ubiquity as a feature of the ICT environment. Diversification, however, may entail tradeoffs in cost, performance, interoperability, and even security. New technologies that introduce heterogeneity *within* protocols, software, and software libraries—thus reducing the extent to which a single vulnerability affects all users of a product or service—would be a welcomed priority for future R&D efforts.

IV. PROMISING AREAS

We endorse a technology-neutral approach to cybersecurity and welcome any emerging technologies that prudently support the objectives listed in section III of this comment and Section 201 (a)(1) of the *Cybersecurity Enhancement Act of 2014*. However, in response to question #2 of the RFI, we highlight the following areas as worthy candidates for additional emphasis in cybersecurity-oriented R&D programs:

- **Encryption.** Notwithstanding wide use of encryption in computing generally and cybersecurity specifically, advancements in—and innovative applications of—encryption could still improve security in a variety of areas. Basic and applied research should continue to this end.
- **Verification and certification**. Advancements providing for automated formal verification and certification processes for computer operating systems and software have the potential to drastically reduce or eliminate security vulnerabilities that are, at present, so prevalent and frequently exploited. R&D to this end should be emphasized and resourced accordingly.

V. ADDITIONAL NOTES

We encourage R&D planners to also take into consideration the following points:

- **Sustainment**. A consistent, multiyear approach to R&D is far more likely to yield positive outcomes than unpredictable, ad hoc support.
- **Transfer**. Commercializing R&D is critically important in order to realize a return on investment. BENS encourages R&D-related partnership and transfer arrangements that are open, clear, and competitive.
- **Flexibility**. With recognition that norms related to security—as well as the legal and regulatory framework governing security practices—will continue to evolve and change over time, cybersecurity R&D should be pursued in a fundamentally open, flexible, and tolerant environment.