Dear [SPONSOR]:

In connection with the research project(s) on the enclosed list, we write to notify you of a compromise to the University’s College of Engineering computer systems.

The University and its forensic experts have conducted a thorough analysis of the College of Engineering’s computer network to determine the full scope of the security breach and have taken steps to restore the integrity of the college’s systems. Although we felt it prudent to alert you to this issue, we do not have any specific indication that data related to the research project(s) on the enclosed list has been compromised.

The University values its working relationship with [SPONSOR AGENCY], and takes seriously the security of its systems. To that end, we write to provide you with information concerning the nature and extent of—and the full response to—the compromise.

In late November 2014, the Federal Bureau of Investigation provided a victim notification report to the University relating to suspicious cyberactivity directed at certain systems and computers in the College of Engineering. Penn State immediately launched a comprehensive internal investigation into the FBI’s report and retained leading third-party computer forensic experts to assist in the investigation.

The University immediately retained cybersecurity experts to analyze the College of Engineering system for the existence, nature, and scope of any cyberthreat, and by December 2014, the University was advised that several systems in the College of Engineering were the targets of highly sophisticated cyberattacks, often referred to as an Advanced Persistent Threat. In such an attack, threat actors orchestrate covert targeted attacks to gain access to a system and then employ sophisticated evasion techniques to remain undetected, sometimes for years. In this situation, there are indicators that suggest computer systems in the College of Engineering may have been attacked as early as September 2012, and that the intruders used sophisticated evasion techniques to remain undetected. In January 2015, the University retained Mandiant, a foremost leading cybersecurity firm, to perform additional analysis of the cyberattacks, and to assist in planning remediation of the compromise.

Mandiant completed its analysis of the systems on May 15, 2015, and a large-scale, coordinated remediation of the College of Engineering system is now underway. Consistent with standard industry practice, the existence of the threat and the response has been kept in the strictest of confidence in order to ensure the security and integrity of the system and maximize the likelihood of success of the remediation. This confidentiality has been essential in order to eradicate the threat actors without providing them with an opportunity to establish an unknown foothold within the system only to be reactivated after remediation—or to identify new pathways into the network. Mandiant and University personnel have analyzed the extent of the threat, and as of May 15, 2015, are executing remediation. To the best of our knowledge, this has been done
without having alerted the threat actors beforehand. With Mandiant’s assistance, we have also taken significant steps to fortify the college’s cybersecurity defenses. These measures will continue to provide the University with even greater capability to prevent, detect, and respond to cybersecurity issues.

We are, of course, happy to answer any questions you might have, or provide you with any additional information you might seek. Such answers and additional information about the analysis and the remediation may be found in Mandiant’s summary, which we have enclosed for your convenience, and at http://SecurePennState.psu.edu. Please also do not hesitate to contact my office at VPRnotification@psu.edu or 814-867-6367 with any additional questions or requests.

Very truly yours,

Neil A. Sharkey, Ph.D.
Vice President for Research

Cc: