**********DRAFT EMAIL TO BOARD OF REGENTS ON SOLAR WINDS **********
To: BORMembers List
Cc: All to and cc addees above
Subj: [redacted] Cyber Activity Alert

[redacted]

Board of Regents,

Good Afternoon. I am making you aware that the global compromise of SolarWinds that you have likely heard about in the news has potentially impacted some of our campuses information technology (IT) environments. SolarWinds assets are used to manage our servers and networks and as a result, these assets have broad access and high privileges to the rest of our IT environment. Recently, the Cybersecurity and Infrastructure Security Agency (CISA) issued an alert which describes the threat in great detail. We have shared this and other threat intelligence with our campuses. The investigation is ongoing to determine the full extent and impact of the threat to our institutions.

***Global Context*: This particular compromise is part of a global campaign to infiltrate public and private organizations through "trojanized updates" of the SolarWinds Orion IT monitoring and management software. It is estimated this incident was likely the result of a highly sophisticated, targeted, and manual supply chain attack by an outside nation state. This campaign may have begun as early as Spring 2020 and is currently ongoing. The most dangerous effects of this campaign are lateral movement within infiltrated networks and the exfiltration of data from the compromised networks.**

What We Know

1. We have begun the investigation at our 13 campuses plus technology environments for UWSA/UWSS and UW-Extended Campus.

6 of our 15 institutions do not use SolarWinds products and are not impacted.

- 4 of our 15 institutions use Solar Winds but older versions that have been reported as impacted. These institutions have upgraded their systems to a clean, post-infection version and can resume use as necessary.
- 3 of our 15 institutions use the impacted version of SolarWinds but have not found the presence of any malicious code. These institutions have disconnected systems; patched their systems with the vendor-provided fix; and searched for indicators of compromise that might indicate infection.
- 2 of our 15 institutions [redacted]
- [redacted]
- [redacted]
- [redacted]
- Estimated number of individuals impacted / records exposed: TBD
- Status of investigation: In progress

- [redacted]
- [redacted]
- [redacted]
- Estimated number of individuals impacted, or records breached: TBD
- Status of investigation: In Progress

Additional Actions Taken:
I have directed the Chancellors to take specific actions from the CISA guidance and report back to UWSA when complete. This also includes actions to all institutions regarding tangential attacks not related to SolarWinds that could be impactful. I am getting daily updates from my Office of Information Security as the investigation continues.

I will keep you apprised of new information as it becomes available.

Tommy

Tommy G. Thompson
President