**********DRAFT EMAIL TO CHANCELLORS ON SOLAR WINDS **********
To: Chancellors List; CIOs Only cios_only@uwsa.edu
Cc: All to and cc addees above; Lori Storz; and UW Technical Information Security Committee uwtisc@uwsa.edu

Subj: [redacted] Cyber Activity Alert

[redacted]

Chancellors and Chief Information Officers,

Good Afternoon. I am aware of the global compromise of SolarWinds and the potential impact to our 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 U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued the attached alert which describes the threat in great detail. At this time, we know that some of our campuses have been impacted. The investigation is ongoing to determine the full extent and impact of the threat to our institutions. As the CISA alert states, “This is a patient, well-resourced, and focused adversary that has sustained long duration of activity on victim networks”.

As a result of the seriousness of the threat, I am directing all Chancellors to take the following actions to secure their campus technology environment.

- All institutions:
  - CISA is investigating attack activity that does not leverage SolarWinds Orion, or where SolarWinds Orion was present but there was no SolarWinds exploitation activity observed. Such attacks include bypassing Duo multi-factor authentication to access web-based email. As a result every UW institution should:
    - Run the Microsoft supplied queries to check for malicious activity in their directory services environment (p. 4)
    - Check for "impossible travel" logins in your environment (p. 5)
    - Check for "impossible tokens" in your identity services environment (p. 5)
      - Please report planned completion date of these actions to the Office of Information Security by end of day, December 23, 2020.
- All SolarWinds institutions:
  - If you have a vulnerable SolarWinds Orion product in your environment (see the attached CISA alert for product details in Appendix A):
    - Identify your category (p. 6)
    - Take the appropriate mitigation steps (p. 7)
  - Please report your category and planned completion date of appropriate mitigation actions to the Office of Information Security by end of day, December 23, 2020.

I have asked the UW System Office of Information Security (OIS) to follow-up with each institution to confirm the completion of actions, any assistance required, as well as to determine appropriate next steps based on the findings.

Thank you for your attention to this important matter.

Tommy

Tommy G. Thompson
President
1720 Van Hise Hall, 1220 Linden Dr
Madison, WI 53706
608-262-2321 | wisconsin.edu