Motivation
The proposed system and network security policies provide the foundation to implement a cybersecurity program at SIO that is tailored to the advanced threats the institution faces from foreign state actors.

It is important to point out that all of the individual requirements contained in the two documents are taken from the campus and system-wide cybersecurity policies and technically already apply to SIO. However, these higher-level policies are so broad in scope that they don't map well to the needs of a research-oriented unit such as SIO.

The proposed policies call out those requirements that provide the most protection in SIO's complex IT environment. The vast majority of the measures are actually already implemented across many areas of SIO and have been deployed without interfering with ongoing research activities. Adopting them as policies removes any remaining doubt that they need to be implemented wherever possible. (Both the network and the system security policies contain provisions for exceptions to the standards when warranted to support unique equipment.)

The documents also fulfill the UCOP Electronic Communications Policy (ECP) requirement that "Providers of electronic communications … document and make available to their users general information about these monitoring practices".

Finally, the adoption of the policies would also show that the institution cares about defining and improving its cybersecurity posture. They can be provided to our sponsors to document our ongoing efforts, over and above the more generic policies from the campus and the UC system.

Summary
The proposed SIO networking and system security policies protect SIO in the areas listed below. All of the requirements are risk-based and their implementation in each area will depend on the sensitivity of the data and the work being done. Obviously, groups that handle or create information with higher sensitivities need to expect even tighter restrictions as defined by outside agencies.

Stopping bad actors

- Block known attacks and bad actors into SIO networking
- Monitor outgoing traffic for known indicators of compromise
- Block commonly abused protocols except when needed

Using known good tools

- Install standard campus and SIO provided security software
- Configure public servers with standard secure settings
- Allow security status verification by standard campus and SIO tools
- Use standard campus services except when needed

Documenting important data

- Maintain inventory of systems and any important data they contain
- Track computers or devices that have non-standard security configurations
- Notify SIO management when incidents occur