Massachusetts Institute of Technology

Israel Ruiz
Executive Vice President and Treasurer

Office of the Executive Vice President and Treasurer
Building 4-204

77 Massachusetts Avenue
Cambridge, Massachusetts
02139–4307

Phone 617–253-4495
Email iruiz@mit.edu
http://web.mit.edu/evp

April 2, 2013

To Members of Academic Council:

The recent hoax incident of February 23 and hacks to MIT's information network have given us the opportunity to reassess our emergency preparedness, emergency communication protocols, and network security practices. Today I want to share with you the improvements we are making to our systems and procedures to ensure the safety of our community and the integrity of our campus. I ask that you disseminate this information throughout your respective areas, so that we can build awareness of the important enhancements we are pursuing.

Safeguarding our community

We have upgraded our emergency-preparedness training program, and are reaching out to all parts of our community through our Security and Emergency Management Office (SEMO). ***It is critical that each department, laboratory and center (DLC) have an emergency coordinator and a concrete emergency plan.*** SEMO staff will connect with DLCs to provide guidance in crafting and communicating these plans, to share training materials and provide in-person training.

We are also working with housemasters in our residence halls and staff members in the Office of the Dean for Student Life to strengthen the safety of our students and enhance the preparedness of our dormitories and fraternities, sororities and independent living groups (FSILGs).

Reaching people in an emergency

We have revised our emergency communication protocols so that we are able to notify people within minutes of an emergency situation, and are working to expand our addressable alerts system to include all members of our community on all devices. We currently send text-message alerts to all Institute owned mobile telephones and email to all MIT email addresses.

In addition, approximately 60% of our faculty, students and staff have elected to participate in MIT's alert program so that they may receive alerts through personal mobile telephones and email addresses. ***We will be sending email to those who have not yet signed up to urge them to participate in this expanded system of alerts, so that we are able to reach everyone quickly in the case of an emergency.***

Improving MIT's cyber security

With guidance from CSAIL Professor Frans Kaashoek, who serves as technology domain expert for the Information Technology Governance Committee, we have examined how we deliver network services to our community. We have determined that we can modify practices to establish a higher level of resilience for our network while accommodating the needs of our faculty, students and staff.

MIT has a long history of operating an open network environment, allowing devices on MIT's network unrestricted incoming and outgoing access to the Internet. The Institute remains committed to providing open Internet access to support the core mission of teaching, learning and research, while also providing a more secure network environment for our community.

In order to provide the community with a more secure network environment, Information Services and Technology (IS&T) will soon implement several changes to our network. For most of the MIT community, particularly those engaged in research, teaching, and learning activities, these changes to our network will be invisible. Connections to MIT's communications (email and Web) and academic services (Stellar and WebSIS) will not be impacted. Some administrative users, particularly those who work while away from campus, may see changes to how they interact with MIT's administrative systems. Questions about planned changes highlighted below can be directed to cybersecurity-questions@mit.edu.

- Network traffic policies are being strengthened. By default, traffic originating from outside MIT's network (from non-MIT IP addresses) will be blocked to reduce the potential for damage to MIT information systems. This will not impact open services such as email and publicly accessible websites.
- Access to MIT administrative applications such as the Data Warehouse, SAP and MITSIS will require connecting from MIT's network on-campus (from MIT IP addresses) or by making use of MIT's virtual private network (VPN) service.
- MIT will implement stronger password quality and expiration policies.
- Those engaged in research, teaching and learning activities will be given the option to opt out of the default network security policy through a self service mechanism.
- Community members requiring access to their computer systems from non-MIT IP addresses are encouraged to use MIT's VPN service for access rather than opting out.
- Individuals whose work involves access to legally protected or otherwise sensitive information are advised to take additional precautions on devices used for confidential data access, such as use of two-factor authentication and full-disk encryption.

I am deeply and personally committed to safeguarding our community, protecting our campus and securing our systems. Together with our colleagues dedicated to campus safety and security, with the support of senior academic leadership and in collaboration with the campus community, we are deploying all necessary resources to this effort. It will require the dedication of all of us to promote safety awareness, complete necessary emergency training, and adhere to reinforced cyber security guidelines. IS&T staff members are working with information technology (IT) leadership and partners across campus in making the changes described above. We continue to explore all opportunities to further strengthen our preparedness, and will communicate additional information as these plans evolve.

Sincerely,

Israel Ruiz