

Comments By: Jim McCoy, Capital Design and Construction Department

Prepared For: Virginia Tech Review Panel

Date: May 21, 2007

### **Building Security, Mass Notification and Emergency Procedures**

Good morning. My name is Jim McCoy and, as President Steger indicated, my presentation this morning will focus on the university's building security infrastructure, mass notification systems and emergency procedures that were in place prior to April 16, 2007. While other presenters will speak in detail later this morning about the events of April 16<sup>th</sup>, this presentation is intended to provide Panel members with a brief overview of the pre-existing framework and operational procedures that relate to those events.

Building perimeter security for campus facilities is primarily confined to lockable exterior doors. With minor exceptions, building access is controlled by electronic card readers or conventional locks and keys. Access to interior spaces is controlled in a similar fashion. For discussion purposes, it is useful to categorize campus buildings into two groups, Student Housing facilities and Academic/Administrative/Support facilities.

There are forty-four Student Housing facilities on campus which house 9000 students. For these facilities, perimeter building access is controlled by electronic card readers which are managed and maintained by the Hokie Passport Office. The Hokie Passport, which serves as a student's identification card, is a magnetic stripe card that can be used for multiple purposes such as to purchase meals and services, to gain access to recreational sports activities and to obtain tickets to athletic events. With respect to building security, the card allows a building resident to access only their particular building during such times that the exterior doors may be locked. The electronic system can lock exterior doors on a scheduled or an as needed basis. Typically, Student Housing facilities are locked between the hours of 10:00 pm and 10:00 am each day. During all other times, the buildings are unlocked and fully accessible. It should be noted that entry doors to Student Housing facilities are not monitored at any time. As such, even during times when the doors are locked, non-residents can gain access by "tailgating" when an actual resident enters or leaves the building.

Access through interior doors within Student Housing facilities, including doors to resident rooms, is typically controlled by institutional locks and keys. Key issuance and control is managed by the Office of Student Programs.

With a few exceptions, perimeter access to Academic/Administrative/Support facilities is controlled by institutional locks and keys. These buildings are typically unlocked between the hours 5:30 and 6:00 each weekday morning by custodial personnel, and remain unlocked and fully accessible throughout the day. Based on a locking schedule that begins at 5:00 pm and continues through 11:00 pm to accommodate evening classes, a university security crew locks the exterior doors of these buildings. Most buildings remain locked throughout the weekend. Building occupants, who may need to access the building during such times that the exterior doors are locked, may be issued exterior door keys from the Key Control Office within the Physical Plant Department.

Depending upon the function of the space, interior doors may or may not be lockable. Many classrooms and public areas have doors that can be locked, but only from the public/corridor side using an appropriate key. Typically, these doors remain unlocked because of the constant use of these types of spaces. Classrooms, for example, also serve as meeting rooms for a multitude of student organizations during "off" hours. Continuous use by multiple parties for a variety of functions makes controlling access to classrooms impractical. Private offices, building support spaces (Mech/Elect Rooms, Telecommunications Rooms, etc.) and laboratory spaces are also lockable. Conventional locks and keys are typically used to secure and access these spaces. In some buildings, certain interior spaces are secured with electronic card readers or biometric devices. These particular spaces have a heightened level of security which reflects the need to control access more tightly.

There are currently two systems on campus which provide for mass notification. The Emergency Alert System consists of pole and roof mounted speakers at six locations throughout the campus. This system allows for an audible message, either voice or tone, to be broadcast from the controller which is located in the Virginia Tech Police Department. When activated, this system allows for emergency messages to be conveyed to individuals who are on campus, but not within a building. On April 16<sup>th</sup>, four of the locations were operable and the other two locations were in the process of being installed.

Depending upon which building they are in, building occupants may receive an emergency message through the building's fire alarm system. There are currently over one hundred buildings on the Virginia Tech campus, including all Student Housing facilities, that are equipped with a fire alarm system. The systems serving forty-one of these buildings also provide voice alarm capabilities if delivered from the building's fire alarm panel. While enhancements are needed to centralize this function which will make it a more viable alternative for mass notifications, much of the infrastructure is already in place to notify a significant portion of the university community in the event of an emergency.

For many years, the university has maintained an Emergency Response Plan. The current plan, which has been in place since May 2002, provides a set of protocols for dealing with campus emergencies of varying degrees. The priorities of the plan are 1) to protect life safety, 2) to secure critical infrastructure and facilities and 3) to resume teaching and research programs. This plan provided the framework by which university officials mitigated, responded to and began recovering from the events of April 16th.

At the crux of the plan are the actions and interactions of the two pre-established functional groups. The Policy Group, made up of senior administration, creates the policies and procedures needed to support emergency operations. The Emergency Response Resource Group, comprised of the leaders of various university departments whose services are responsive to the event, implements the procedures set forth by the Policy Group.

Once activated, the plan encompasses many activities, including the timely dissemination of accurate information. As it becomes available, information about an event is gathered by the appropriate plan participants and channeled back to a command center where the Policy Group establishes a plan of action based on the information being provided. At the appropriate time or times, other plan participants communicate applicable information about the event to the campus community and beyond. As prescribed by the plan, these communications can take many forms including broadcast email, broadcast voicemail to campus phones and updates to the university homepage. Where appropriate, communications through the Emergency Alert System and available building fire alarm systems may also be enacted.

As the events of April 16<sup>th</sup> are detailed in a later presentation, I am confident that the Panel will see the correlation between the actions of university officials that day and the Emergency Response Plan that was in place at the time.

With that, I'll conclude the presentation. If, however, there are questions from Panel members regarding the university's security systems or emergency procedures prior to April 16<sup>th</sup>, I'll be happy to try and answer them for you at this time.