Executive Summary
April 15, 2006
Escape from the Minnesota Sex Offender Program
***Investigation status through May 12, 2006**

Incident Summary
On April 15, 2006, at approximately 9 p.m., unit staff discovered that four patients of the Minnesota Sex Offender Program (MSOP) in St Peter had escaped from the South Unit. The patients escaped by removing a bar from the security window in a patient room, breaking out a portion of security glass, and lowering themselves to the ground by a rope fashioned by tying a hand-made belt and bed sheets together.

Law enforcement was contacted immediately upon the discovery of the escape, and was in charge of all efforts to capture the escaped patients. Three of the four patients were apprehended by law enforcement in St. Peter within hours. Staff of the Special Investigations Unit in State Operated Services (SOS) worked cooperatively with multiple local, state, and national law enforcement agencies to capture the one patient who remained at large until apprehended by law enforcement in Kansas City, Missouri, on May 2, 2006.

On April 16, 2006, SOS initiated an internal investigation to identify the factors that contributed to the escape. The internal investigation involved staff interviews, policy and procedure review, and examination of the physical plant, including all components of security that were breached during the escape.

Audit of Existing Security Components
The investigation examined policies and procedures, staffing levels, the electronic perimeter monitoring system, and the integrity of the window bars and security glass associated with the security breach. The investigators concluded:

- Policies and procedures were adequate. Had the policies and procedures been followed, the escape would have likely been discovered and thwarted.

- Staffing levels on the South Unit and in the MSH Control Center were adequate.

- The window bars and security glass were adequate. Due to the window bar design and materials used in the fabrication, it would require weeks to cut through the bar. Breaking of the security glass would have taken time and would have created considerable noise. These components were breached due to staff not completing required window checks and not being actively engaged with the patients on the unit.

- The electronic perimeter monitoring system, when activated, was sufficient to have alerted staff in the control center to the breach of the bars and window. The perimeter security system had been deactivated by staff contrary to established policies and procedures.

Factors Contributing to the Security Breach:
The investigation concluded that the direct cause of the security breach was staff failure to comply with policies and procedures in both the South Unit and the Minnesota Security Hospital (MSH) Control Center. Systemic issues, although not direct factors in the escape, contributed to the environment that led to the security breach.

Staff Non-compliance
1) South Unit

- South Unit staff did not properly follow policies and procedures prescribing how to effectively conduct window security checks, monitor patient property, and monitor for the introduction of contraband.

- South Unit staff were not out on the unit actively engaging patients, assessing behavior, and reporting potential problems.

- There was insufficient supervision of staff's performance of security checks and interactions with patients.

- South Unit staff failed to report suspicious patient behavior to the Office of Special Investigations and failed to follow up on reports of suspicious behavior by the adjacent North unit staff.

Minnesota Security Hospital (MSH) Control Center

- MSH Control Center staff failed to follow policies and procedures on reporting of system malfunctions, requests for system maintenance, and authorization to shut down electronic monitoring systems.

- Control Center supervisory staff failed to adequately monitor control center policies and procedures, particularly the proper use of electronic security systems.

Systemic Issues
Although not direct factors in the escape, the following issues contributed to the environment that led to the security breach. However, with programmatic and security enhancements to address the systemic issues, there will be added redundancy in the system that will guard against staff failure in the future.

- The presence of the MSOP and MSH populations on the same campus, the sharing of facilities and staff to serve these population, and the number of policy changes being implemented for MSOP created difficulty and confusion in applying the relevant security policy and procedures.

- The majority of line MSOP staff and unit managers have less than 2 years experience.
- There was no preventative maintenance schedule for the electronic monitoring system.
- Patients report that some staff exhibit disrespectful behavior toward the patients, while staff report patients have exhibited threatening and intimidating behavior.
- All patients, including those not participating in treatment, require more structure and opportunities for activities in their daily routines.
- MSOP patients at all levels of the program are frustrated by a perception that there is not a way to get discharged from the program.

Corrective action

The corrective action plan is anticipated to be completed by the end of May, contingent upon conclusion of the investigation. Corrective action in certain areas has been identified and in some areas initiated. However, because the investigation is still in progress, the following actions are not all-inclusive.

- Staff corrective discipline has been initiated.
- Structural organizational changes will be made that will clearly delineate security responsibilities.
- Department of Corrections security policies and procedures will be implemented.
- All aspects of MSOP programs will be segregated from MSH programs.
- Program improvements will be made by establishing an overall structure that produces predictability and consistency in patients' daily routines and interactions with staff.

This Executive Summary does not include confidential personnel information, security information, or private patient information.