STATEWIDE TERRORISM & INTELLIGENCE CENTER
STANDARD OPERATING PROCEDURES
SOP-007, INTERNET & EMAIL USAGE

I. POLICY

The Statewide Terrorism & Intelligence Center (STIC) is a 24 hour/7 day a week call center which provides immediate intelligence information to local, state, and federal law enforcement agencies on suspects of terrorism and major crimes incidents. STIC will establish a minimum staffing policy to insure STIC maintains an adequate staffing level to function efficiently. No person at STIC using the Internet via an Illinois State Police (ISP) connection has any proprietary interest or expectation of privacy in the use of the Internet. All persons using ISP's connection to the Internet are subject to having their usage monitored by the ISP at any time and without notice.

II. DEFINITIONS

II.A. Terrorism Research Specialist (TRS) - Full-time Illinois State Police Code employee who researches and analyzes data in regard to potential terrorism suspects and incidents which may be precursors for terrorist activity.

II.B. Criminal Intelligence Analyst (CIA) - Full-time Illinois State Police Code employee who primarily researches and analyzes data in regard to criminal activity, suspects, and incidents.

II.C. Internet - a global web connecting computers. Unlike online services, which are centrally controlled, the Internet is decentralized.

II.D. E-mail - a means of communication using commonly accepted e-mail software and protocols which electronically convey information, including text and attachments from one person to one or many persons. For the purpose of this directive, e-mail does not include other forms of electronic communications such as Illinois Wireless Information Network (IWIN) Messaging and NLETS/LEADS Administrative Messages, which will be addressed in other ISP directives.

II.E. Intranet - the collection of ISP internal inter-connected networks which use TCP/IP protocols.

II.F. Lotus Notes - the electronic message platform currently sanctioned and supported by the ISP.

II.G. User - The user is any person who has been authorized to read, enter, update, or disseminate information by the owner of the system or application data.

III. RESPONSIBILITIES

III.A. The Statewide Terrorism & Intelligence Center (STIC) will allow and encourage the use of Internet services to support the various missions of the Department. Use of the Internet requires responsible judgement, supervisory discretion, and compliance with applicable laws and regulations. Users must be aware of information technology security and other privacy concerns. Users must be aware of and follow management directives for Internet usage.

IV. PROCEDURES

IV.A. ISP's Internet service must not be used to:

IVA1. communicate information that is illegal or unrelated to ISP's mission or

IVA2. access chat rooms or instant messaging unless doing so is required as part of a Departmental investigation.

IV.B. ISP is aware that Internet e-mail may not be confidential and may in some instances be used as evidence in court cases.

IV.C ISP reserves the right to examine the content of the hard drive and any other component of any state-owned computer to inspect for unauthorized software and to examine e-mail and data for unauthorized use. Except to the extent that may be required by law and as may be specified by ISP policy, there is no expectation of privacy for information maintained by or transmitted through state-owned computers.

IV.D. Since the Internet does not conform with the security standards established for the state's protected information resources, sensitive or confidential information must not be allowed to flow unprotected through the Internet environment.

IV.E. Use of the Internet can provide a number of benefits to the ISP, such as access to a vast amount of information and access to an increasingly large number of experts and specialists in law enforcement related fields.

IV.E.1. ISP employees may use ISP Internet service for this purpose if such use is related to their duties.

IV.E.2. Incidental use, such as accessing weather information or reviewing news updates, is permissible but only to the extent it does not disrupt

the employee's regular duties and is authorized by the work location supervisor.

IV.F. Each individual using the Internet must do so responsibly and professionally.

IV.F.1. In case a specific use is not identified within this directive, the principle to follow in determining if a use is acceptable is if the use is ISP business related and will provide a work related benefit to the user.

IV.F.2. If these conditions cannot be met, the use should be considered not acceptable.

IV.F.3. Users that encounter illegal activities or inappropriate solicitations via the Internet must immediately report such activities to their supervisor and to Security Administration, the Bureau of Infrastructure Services (BIS), Information and Technology Command.

IV.G. The following deliberate uses of the Internet are considered to be unacceptable:

IV.G.1. any use that is disruptive or in any way detracts from the effective operation and management of the workplace.

IV.G.2. receipt or transmission of any materials in violation of any government laws, use for a for-profit activity or use for private or personal business.

IV.G.3. the use of obscene, abusive, pornographic material or objectionable language or images in either public or private messages.

IV.G.4. the sending of messages or files that are likely to result in the loss of the recipients' work or systems.

IV.G.5. the sending of chain letters or broadcast messages or any other type of use that would cause congestion of the network or otherwise interfere with the work of others such as streaming audio and streaming video, unless part of official duties.

IV.G.6. gambling.

IV.H. Users will access and monitor their Lotus Notes messages and calendar on a daily basis during their normal work hours, use Lotus Notes message system equipment in an authorized, safe, and legitimate manner, monitor their Lotus Notes files and retain

and purge the files, as appropriate, change their Lotus Notes password monthly, change their RACF password monthly and ensure they fill out Company, Work Phone Number, Work Location and Manager fields in the Notes Address Book.