Security Plan for Document Reviewers

David Wagner, Principal Investigator, University of California, Berkeley

1. Compliance with this security plan is mandatory for all document reviewers.

Secure facilities

2. Each site will have a room or rooms where the work is to be performed. Access to the room will be limited to project participants. The room will be kept locked at all times.

3. Keys or access codes to the room will be made available only to authorized document reviewers or Principal Investigators, and only after they have signed the relevant Confidentiality Agreement, the Acknowledgement of Statement of Work, and the Security Plan. Keys or access codes may also be made available to trusted staff but only as necessary (e.g., fire marshals). A log will be kept of everyone who receives a key or access codes to the room.

4. Exception to Item 3: If it is not possible to restrict access to keys or access codes to the room as outlined in Item 3, then the following additional restrictions apply:

- The facility will have a safe or other security container inside the room.
- The combination to the safe will be made known only to authorized document reviewers or Principal Investigators, and only after they have signed the relevant Confidentiality Agreement, the Acknowledgement of Statement of Work, and the Security Plan.
- All working notes, proprietary documents, and print-outs will be stored in the safe when the room is unattended.
- Desktop PCs will be equipped with external hard disks. Team members will exercise reasonable caution to ensure that all proprietary or confidential information is stored only on the external hard disk, not on the PC's internal hard drive. External hard disks will be stored in the safe when the room is unattended.

These additional restrictions do not apply if the requirements in Item 3 are met.

5. The room will contain dedicated desktop PCs which may be used for processing documents. Documents will not be installed on other machines.

Labeling

6. The facility will use strict "air-gap" security and military-style red-black separation. The PCs in the room may be networked to each other as long as the network does not extend beyond the premises of the room at any time. PCs will have no wireless capability.

7. Removable storage media (e.g., USB dongles, CD-Rs, DVD-Rs) will be labeled Confidential once proprietary or confidential document or information has been installed on them. Removable storage media that has been labeled Confidential will not be removed from the room.

8. Proprietary documents, print-outs, and other paper documents containing proprietary or sensitive material will remain in the secure room and will not be removed from it. In the case where teams use two adjoining secure rooms for their work, print-outs and working notes may be hand-carried temporarily from one secure room immediately to another so long as they remain under that person's tight personal control while they are transported.

9. For purposes of enabling secure transmission of working notes, draft reports, or other sensitive data from one secure facility to another, or for enabling secure off-site backups of this data, the following procedure may be used. The data will be encrypted using a cryptographic-strength program, such as GPG/PGP, with a high-security key or passphrase. It will then be written in encrypted form onto a CD-R or DVD-R, which will be marked as confidential. The disc may then be removed from the premises and couriered hand-carried to its destination. The cryptographic key or passphrase will be kept separately from the disc and will be disclosed only to authorized team members and only via telephone or in person. Discs will be destroyed as soon as they are no longer needed, or upon completion of the project.

Intranet

10. Team members can use any network applications they like on the internal network among PCs, including but not limited to email, chat, Wiki, shared document repositories, etc.

Personal laptops

11. Team members may bring laptops into the facility, subject to the following restrictions.

12. Proprietary documents provided by the State will never be installed on laptops.

13. Laptops may be connected to the Internet via an external wireless network, but they may not be networked to any other machine.

14. Team members may use removable storage media (e.g., CD-Rs, DVD-Rs, USB dongles) to transfer files from laptops to PCs in a unidirectional fashion. Read-only media are preferred for this purpose. However, files shall not be transferred from PCs to laptops.

Communication

15. Team members may communicate over the Internet with other project participants about proprietary or confidential matters *only* in the form of email encrypted using GPG/PGP. Other forms of Internet communication will not be used except for messages containing no proprietary or confidential content (e.g., to schedule a phone call).

16. Team members may use telephone to communicate with other project participants.

17. Team members will avoid discussing proprietary or confidential information in public spaces where others might potentially overhear.

Completion of the project

18. Upon completion of this project, all storage media, devices, and PCs that may contain confidential or proprietary material will be securely erased or destroyed, before they are removed from the room (e.g., to ship them back to the Secretary of State).