

**National Science Foundation / U.S. Navy Memorandum of Agreement
on Ocean Observing System Security**

Annex B

**Standard Operating Procedures for Security Issues Posed by Ocean Bottom
Seismometers**

1. INTRODUCTION

- 1.1. Ocean Bottom Seismometers (OBSs) are non-cabled, bottom-deployed observational instruments equipped with sensors to monitor seismic activity of the seafloor. The sensors continually record the movement generated by tectonic plate activity on an internal storage disk that is processed only upon retrieval of the OBS. OBSs, including OBSs supplemented with hydrophones, have the ability to collect data of interest to the U.S. Navy and thus present a potential threat to U.S. national security. Accordingly, it is necessary to establish appropriate procedures to mitigate this threat.
- 1.2. Intent: The National Science Foundation (NSF) agrees the U.S. Navy must protect from public release certain data of interest that might be collected by ocean-deployed OBSs. The U.S. Navy agrees OBS data are invaluable to the scientific community and should not be unnecessarily restricted from release. The NSF funds Principal Investigators (PIs) to conduct science experiments using OBS instruments. NSF agrees to allow the U.S. Navy to take custody of and screen OBS data that could potentially have a negative impact on national security if made public. The U.S. Navy agrees to safeguard all data in its custody, keep only that data that must be retained for national security reasons, and return all other OBS data as quickly as possible.
- 1.3. To allow efficient and effective coordination among Participants, this Standard Operating Procedure (SOP) for OBS experiments defines activities necessary to mitigate the potential risk to national security. During the experiment planning stages, the SOP will establish appropriate mitigation plans and processes, ensure open communication among the participants, and provide lead time to allow necessary actions by all concerned in a timely manner. During the experiment deployment, recovery and data processing phases, this SOP will allow the participants to maintain configuration control of the plan and to implement the agreed upon security procedures to permit efficient screening of data of interest and timely release of cleared data.

2. STANDARD OPERATING PROCEDURE (SOP) MECHANISMS

- 2.1. Participants: The Chairman of the U.S. Navy's Ocean Observing System Security Group (OOSSG) will represent the U.S. Navy's interests in discussions with the NSF regarding OBS experiments funded by NSF. Mr. Bauke Houtman will represent the NSF's interests in OBS experiments.
- 2.2. Meetings: The OOSSG and NSF will communicate as necessary to resolve issues regarding OBS experiments under the NSF's purview. Early visibility into and review of NSF-funded OBS experiment plans by OOSSG members will allow identification of potential national security issues, whether technical, procedural or policy related, and will facilitate resolution.
- 2.3. NSF and the OOSSG will institute a mitigation plan for each NSF-funded OBS experiment that could pose a threat to U.S. national security. Clearly understood OBS capabilities and placement are critical to the communication and information exchange necessary for this SOP. To the extent possible, NSF agrees to locate sensors so as not to interfere with instrumented Navy training ranges.

The following elements will be included in the mitigation plan. Collection of this information will be coordinated by NSF and maintained by the U.S. Navy.

- 2.3.1. Geographic locations of OBS and associated OBS infrastructure (if any).
- 2.3.2. Timing of OBS deployments.
- 2.3.3. Details of all the technology used, including: the scientific and engineering sensors; additional sensors to be deployed with the seismometers, and encryption of the data.
- 2.3.4. Specifics of the science experiments, including instrument functional specifications, details of the goals of the experiment, and the data to be gathered.
- 2.3.5. A clearly articulated description of the chain of custody for any data to be screened by the U.S. Navy.

Should it be necessary for the OOSSG to review additional details of the technology, NSF will coordinate with the PI and the OOSSG to facilitate such a review.

3. STANDARD OPERATING PROCEDURES

- 3.1. The mitigation process must provide clear and unambiguous awareness of the development plans and deployment status of any OBS experiment. In support of the mitigation process, documents that identify the current status and approval path for each

OBS experiment will be developed. Each OBS experiment will be tracked as it moves from one phase to the next through the mitigation process.

3.2. Pre-Deployment Phase: In the experiment planning stage, NSF will coordinate the collection of required information to help identify and resolve issues early in the process. The following steps will be taken prior to deployment:

3.2.1. NSF will notify each PI, upon selection of their proposal for NSF funding, about data review procedures required to mitigate U.S. national security concerns.

3.2.2. NSF will coordinate the provision of experiment details to the OOSSG. Experiment details include, but are not limited to: a timeline of the experiment; planned geographic coordinates of each OBS; technological capabilities of each OBS; format of the OBS data; any plans to encrypt the OBS data; whether the sensors will be buried; and the anticipated sensor deployment and retrieval processes.

3.2.3. The OOSSG will review the information provided to assess the potential for U.S. national security concerns.

3.2.4. The OOSSG will provide NSF with any requests to modify the experiment plans in response to concerns identified during the assessment process. Each NSF-funded OBS experiment will have a tailored mitigation plan in place before the deployment phase commences. The goal is to reach a consensus agreement among the Participants on the experiment and mitigation plans that supports the science objectives and mitigates any U.S. national security concerns.

3.3. Deployment Phase: Scientific experiments frequently encounter situations which require deviations from the original plan. It is important that all Participants be alerted to any required changes to the plan after the deployment phase has commenced. The following steps will be taken to ensure effective communications:

3.3.1. NSF will remain in contact with the PI during the deployment phase and will notify the OOSSG of any significant changes to the experiment plan (e.g., new geographic location, additional sensors). The OOSSG will review the changes, determine if the changes will affect the mitigation plan, and will provide the results to NSF and the PI.

3.3.2. NSF will provide the OOSSG with final positional information for all deployed OBS units.

3.3.3. The U.S. Navy will inform NSF, who will in turn inform the PIs, of the sensors of interest to the U.S. Navy as soon as possible prior to retrieval of the OBSs.

3.4. Retrieval Phase:

3.4.1. Case 1: When no U.S. Navy representative is onboard the OBS recovery vessel:

3.4.1.1. For OBSs that have not been identified as potentially containing data of interest, there are no restrictions on PI activities.

3.4.1.2. For OBSs that have been identified as potentially containing data of interest, the PIs and OBSIP personnel may follow their normal processing procedures for the OBSs, but must also take the following precautions to safeguard the data. Details of data handling will be specified in the mitigation plan for the project:

3.4.1.2.1. The PI is responsible for controlling access to data of interest until the PI can hand or securely mail that data to the designated Navy representative. All such data must be treated as proprietary data and, after retrieval, stored in a locked desk, locked filing cabinet, locked room, or similar place until custody of the data may be securely transferred to an authorized Navy representative.

3.4.1.2.2. If custody of data of interest is transferred from the PI to other personnel, changes of custody will be tracked in a custody log.

3.4.1.2.3. Upon returning to port, the PI or assigned delegate will account for all media containing data of interest. In general, the data/data media may be handed - or transmitted by first class mail, FedEx, parcel post, or (for bulk shipments) fourth class mail to the designated Navy official.

3.4.1.2.4. It is acceptable to make backup copies of the recorded data to safeguard against inadvertent loss of data, but all copies must be safeguarded and turned over to the U.S. Navy upon return to port.

3.4.2. Case 2: When the U.S. Navy chooses to send a representative onboard the OBS recovery vessel:

3.4.2.1. A U.S. Navy (or U.S. Navy-designated) representative will embark on the OBS recovery vessel and will, upon recovery of any OBS identified as potentially containing data of interest, assume custody of the data storage media removed from that OBS. OBS technicians and other individuals may handle the data media and associated data of interest under the

supervision of the U.S. Navy-designated representative. Where practicable, the U.S. Navy representative will come onboard the retrieval vessel with the pre-designated time windows of data to be screened by the U.S. Navy and will only retain custody of the data from those time windows.

3.4.2.2. When OBSs of interest to the U.S. Navy are recovered, the U.S. Navy representative and Ocean Bottom Seismometer Instrument Pool (OBSIP) technicians will utilize the following general procedures to process the recorded data and provide all data below 4 Hz as soon as possible:

3.4.2.2.1. The OBSIP technicians will record the end-of-deployment time stamp based on a GPS signal for each sensor. The technicians will then remove the data storage media from the OBS.

3.4.2.2.2. The OBS technicians will load the OBS data into a computer, apply a time correction based on clock drift, record other metadata as necessary, and process the raw data into usable format. The U.S. Navy may request that the OBS technician utilize U.S. Navy-provided computers for this processing.

3.4.2.2.3. The U.S. Navy representative will use a Navy-provided computer to low-pass filter the processed data in order to provide all data below 4 Hz to the PI immediately. If technical problems preclude providing the low-pass-filtered data by the completion of the cruise, the U.S. Navy agrees to provide the low-pass-filtered data as soon as practicable.

3.4.2.2.4. Prior to the completion of the cruise, the U.S. Navy representative will provide the original data storage media to an OBS technician or other NSF representative as a safeguard against inadvertent loss of data. The individual must sign an appropriate non-disclosure form agreeing to safeguard the media and to refrain from copying or further processing. The individual will return the original data storage media to the U.S. Navy representative upon receipt of the processed data following post-retrieval screening described in Section 3.5.

3.4.2.2.5. With the exception of the original data storage media and the filtered data below 4 Hz as described above, the U.S. Navy representative will retain custody of all copies of raw and

processed OBS data from the sensors and time periods of interest in order to conduct the Navy's security review

3.5. Post-Retrieval Phase: If required by the tailored experiment mitigation plan, the U.S. Navy will screen the data from the OBS instruments to ensure data of interest is not compromised. The U.S. Navy recognizes the need for timely review and will strive for rapid release of cleared data to support scientific research. Accordingly, the following steps will be taken:

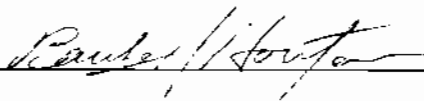
3.5.1 The U.S. Navy will designate the screening facility and inform the NSF as far in advance as possible before OBS retrieval. The Navy will identify sufficient screening resources to ensure all screening is complete within 90 days of return of the recovery vessel to port. Any data not screened within those 90 days will be returned to the PI and NSF.

3.5.2 The Navy screening facility will work as expeditiously as practicable to screen the data and return all data determined to be releasable. The U.S. Navy will work to accommodate any requests to screen and return higher priority data before the full 90 days have elapsed. If the PI or NSF determines any OBS data in U.S. Navy custody involves specific events of interest (e.g., teleseismic events, local earthquakes, tidal conditions, tsunamis, or atmospheric events), the U.S. Navy will make every effort to review that data quickly and return it to the PI and NSF. By returning the data, the U.S. Navy approves of the publication of the data in any form (e.g., journal, web).

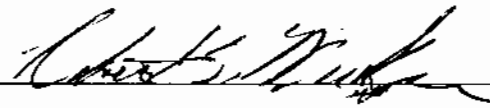
3.5.3 Data the U.S. Navy determines cannot be released to the public will be removed from the data set returned to the PI and NSF. The screening facility will remove only enough data to protect U.S. national security. Data removed from the public data set will be retained by the U.S. Navy in the event the data can be released in the future. The Navy will allow the PI to view any non-releasable OBS data retained at the screening facility.

4. FINANCIAL ARRANGEMENTS

4.1 This Annex will not impose any financial responsibilities on its Participants, except that each Participant will be responsible for the funding costs it incurs in its own interest, related to the support of the Annex.



Bauke Houtman
National Science Foundation
Division of Ocean Sciences
Integrated Programs Section Head



Robert Winokur
U.S. Navy
Chairman, Ocean Observing System Security Group
& Deputy Oceanographer of the Navy

27 JULY 2011
Date

27 JULY 2011
Date