THE SECRETARY OF THE NAVY
WASHINGTON, D. C. 20350-1000

FEB 18 2014

Carolyn N. Lerner, Special Counsel
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 300
Washington, DC 20036-4505

Dear Ms. Lerner,

Thank you for your letter requesting an investigation of alleged danger to public health and safety at Southern California Offshore Range (SCORE), (OSC DI-13-3640).

The Naval Inspector General led an investigation to determine whether the means by which Commander, U.S. Pacific Fleet conducts information assurance activities causes regular disruption to command communications within SCORE, endangering the lives of service members and the general public. The investigation did not substantiate the allegation. Prior to reaching this conclusion, the investigator discussed the evidence with the complainant and the complainant conceded that the facts in the report were true, that the systems were significantly more reliable, and that the establishment of a Range Coordination Center in 2013 addressed his safety concerns.

I am enclosing two versions of the report of investigation. The first contains names of witnesses and is for your official use. I understand that you will provide a copy of this version to the Complainant, the President, and the House and Senate Armed Services Committees for their review.

The second version excludes the names of witnesses and is suitable for release to the general public. As has been the case with other reports that the Department of the Navy has provided to your office since September 11, 2001, I request that you make only this redacted version available to members of the public.

Again, thank you for bringing this matter to our attention. If I may be of further assistance, please let me know at your earliest convenience.

Sincerely,

Ray Mabus
Secretary of the Navy

Enclosures: 1. For Official Use Only Copy of Report
2. Public Release Copy of Report

Office of the Naval Inspector General

OSC Case Number DI-13-3640
NAVINSGEN Case Number 201302910

Report of Investigation

29 January 2014

Subj: Alleged Danger to Public Health and Safety at Southern California Offshore Range

*****

Table of Contents

Suitable for Public Release
(some names removed)

Office of the Naval Inspector General

OSC Case Number DI-13-3640
NAVINSGEN Case Number 201302910

Report of Investigation

29 January 2014

Subj: Alleged Danger to Public Health and Safety at Southern California Offshore Range Arising from Cyber Security Initiatives of Commander, Pacific Fleet

*****

Preliminary Statement

1. This report is issued pursuant to a 27 September 2013 Office of Special Counsel (OSC) letter tasking the Secretary of the Navy (SECNAV) to conduct an investigation under Title 5, United States Code, Section 1213 (5 USC 1213).

2. OSC is an independent federal agency whose primary mission is to safeguard the merit system by protecting federal employees and applicants from prohibited personnel practices. OSC also serves as a channel for federal workers to make allegations of: violations of law; gross mismanagement or waste of funds; abuse of authority; and a substantial and specific danger to the public health and safety.

3. Reports of investigations conducted pursuant to 5 USC 1213 must include: (1) a summary of the information for which the investigation was initiated; (2) a description of the conduct of the investigation; (3) a summary of any evidence obtained from the investigation; (4) a listing of any violation or apparent violation of law, rule or regulation; and (5) a description of any action taken or planned as a result of the investigation, such as changes in agency rules, regulations or practices, the restoration of any aggrieved employee, disciplinary action against any employee, and referral of evidence of criminal violations to the Attorney General.

Information leading to the OSC Tasking

4. The OSC tasking stems from a complaint alleging that the Department of the Navy (DON) Space and Naval Warfare Systems Command (SPAWAR) Systems Center Pacific uses a method of monitoring cyber warfare threats that causes regular disruption to command communications within the Fleet Area Control and Surveillance Facility San Diego (FACSFAC San Diego), and its

detachment, the Southern California Offshore Range (SCORE). The tasker asserts these actions may endanger the lives of service members, DON civilians, and members of the public who may be operating within SCORE.[1]

5. OSC identified the Complainant as Mr. David Richardson, the Technical Director SCORE (hereafter referred to as "Complainant"), and advised that he has consented to the release of his name. The OSC tasking letter stated that Complainant has been employed at SCORE's Operations Center for 27 years and is the principal architect of the SCORE Tactical Training Range System. In this capacity, Complainant and his staff of Electronic Engineers are directly responsible for the safe use of the range.

6. OSC provided the following summary of the Complainant's allegations:

> According to Mr. Richardson, SCORE contains embedded network wiring, which connects and integrates 28 major units of the Pacific Fleet, including radar, hydrophones, threat emitters, live target simulators, and communications systems. All SCORE operations are monitored, controlled, and evaluated in three dimensions and in real time by Operations Center personnel at Naval Air Station North Island.
>
> Mr. Richardson alleges that since 2009, SPAWAR personnel headquartered in Hawaii have created a substantial and specific threat to both Navy personnel participating in fleet exercises in the SCORE range and members of the general public traveling in the vicinity of the range. According to Mr. Richardson, SPAWAR conducts information assurance, including cyber warfare and countermeasures, in a manner which irresponsibly and arbitrarily interferes with the ability of SCORE's Operations Center to maintain the continuous lines of observation and communication necessary during live fire tactical training exercises.
>
> Mr. Richardson contends that in carrying out its cyber security mission, SPAWAR personnel force connections of the

[1] During our preliminary inquiries, we learned the Information Assurance Division of the Communications and Information Systems Directorate (N6) on the Staff of Commander, Pacific Fleet (COMPACFLT), rather than SPAWAR Systems Center Pacific, is responsible for the activities Complainant alleges cause the danger to health and safety of personnel operating within SCORE.

internal SCORE wiring to unsuitable SPAWAR circuits controlled by the Navy Marine Corps Intranet, resulting in an abrupt and complete disruption of both auditory and visual communication between range participants and Operations Center personnel. These communications blackouts occur at least once a day and vary in length from one hour to as long as two weeks.[2] These blackouts result in Tactical Training Range System screens in the Operations Center going blank and the loss of radio voice communications between Operations Center personnel and participating combat ships, submarines, and aircraft. Mr. Richardson compares this situation to a complete loss of visual and auditory communication between an air traffic control tower and approaching aircraft.

According to Mr. Richardson, SCORE receives no notice from SPAWAR of a possible or probable blackout. A blackout results in an immediate and complete disruption of all communication between the Operations Center and range participants. When a blackout occurs, SCORE is forced to wait until SPAWAR, at its discretion, restores communications. Mr. Richardson's attempts to resolve this issue through his chain of command have been unsuccessful.

7. The OSC tasking letter stated the Special Counsel had concluded "there is a substantial likelihood that the information provided to OSC by Mr. Richardson discloses a substantial and specific danger to public safety."

[2] The investigator reviewed with Mr. Richardson the evidence collected from other sources in a follow-up interview on 23 January 2014. This review included statements by other witnesses that complete disruptions of both auditory and visual communications between range participants and Operations Center personnel are substantially less frequent than daily, and last no more than an hour. Mr. Richardson clarified that in his initial complaint he intended to describe any loss of function in the network, even those short of complete disruptions of both auditory and visual communications, and he also intended to include planned, scheduled maintenance periods when the network would be unavailable. If one counted only unanticipated, complete disruptions of both auditory and visual communications between range participants and Operations Center personnel, he agreed with the other witnesses' descriptions of their frequency and duration.

Description of Commands Discussed in This Report

8. FACSFAC San Diego[3] provides off-shore air traffic control and surveillance and active management of DoD airspace, operating areas, ranges, and training resources used to support homeland defense and promote the combat readiness of the U.S. Pacific Fleet and related Joint Forces. It schedules and monitors Navy/Marine Corps training operations conducted off of the Pacific coast and on land ranges in the western United States.

9. SCORE is a detachment of FACSFAC San Diego; the Officer in Charge, SCORE, reports to the Commanding Officer, FACSFAC San Diego. SCORE's geographic area of responsibility includes the waters and ranges in around San Clemente Island off the coast of Southern California, a subset of the area for which FACSFAC San Diego is responsible. SCORE's mission is to improve the combat readiness of Pacific Fleet air, surface, and submarine units in all warfare areas by providing instrumented operating areas and associated facilities to support training exercises conducted within its geographic area of responsibility. SCORE ancillary missions include support for evaluations of equipment and/or tactical concepts developed to support Navy programs. The SCORE Range Operations Center is located on Naval Air Station North Island. The equipment for SCORE's instrumented operating areas is located on San Clemente Island. In August of 2013, SCORE established a Range Coordination Center on San Clemente Island.

10. The Commander, U.S. Pacific Fleet (COMPACFLT) Information Assurance Division (N643) works with COMPACFLT subordinate commands to assist them in complying with computer network security regulations including DD Instruction 8500.2, Information Assurance Implementation, which provides DoD level direction and guidance for computer network security.

11. Commander, TENTH Fleet, is the Navy's Executive Agent for ensuring security of Navy computer networks and compliance with DoD requirements. TENTH Fleet issues regulatory direction and guidance, and provides Information Assurance Vulnerability Alerts (IAVAs), to the administrators of all Navy computer networks via its subordinate activity, the Navy Cyber Defense Operations Command (NCDOC)). These IAVAs direct network administrators to adjust their network operating systems to eliminate security vulnerabilities TENTH Fleet identifies.

---

[3] There are three Fleet Area Control and Surveillance Facilities in the continental U.S. This report will use the term "FACSFAC San Diego" to distinguish it from FACSFAC Norfolk and FACSFAC Jacksonville.

COMPACFLT N643 works with COMPACFLT subordinate activities, including FACSFAC and SCORE, to effect changes necessary to appropriately address IAVAs. Where there is concern that changes necessary to address an IAVA will impair or degrade functionality, COMPACFLT N643 assists subordinate commands to determine if the risk of not making the changes is acceptable.[4]

Description of Conduct of Investigation

12. On 1 October 2012, SECNAV referred the OSC tasking letter to the Office of the Naval Inspector General (NAVINSGEN) for investigation. NAVINSGEN assigned case number 201302910 to the matter and forwarded it to the Inspector General (IG), SPAWAR, for investigation. Two SPAWAR IG investigators who were not subject to the federal agency furlough that went into effect on 1 October 2013 interviewed the Complainant on 3 October 2013 and concluded, with the complainant's concurrence, that the individuals who would be responsible for his concerns are assigned to COMPACFLT N6 rather than SPAWAR.[5] Shortly thereafter, NAVINSGEN reassigned the investigation to the COMPACFLT IG and relieved the SPAWAR IG from further responsibility for the matter.

13. Although NAVINSGEN provided the Deputy Commander COMPACFLT, with a summary of the complaint on 8 October 2013, COMPACFLT IG personnel, who were all civilians on furlough, could not begin working the case until they returned to work on 17 October 2013.

14. On 4 and 5 November 2013, FACSFAC and SCORE personnel briefed the COMPACFLT IG investigator (hereafter the "investigator") on their operations. The complainant also provided a list of 20 individuals (including himself) that he recommended the investigator contact. Based on these briefings and the complainant's proposed list of witnesses, the investigator conducted formal interviews, recorded and under oath, of eight FACSFAC and SCORE personnel and the head of the information assurance Branch for COMPACFLT N6 at Pearl Harbor, HI. The investigator also had informal discussions with eighteen SCORE personnel to learn more about their operations and the matters addressed in the OSC tasker. These informal

---

[4] See footnote 1. The complainant incorrectly stated the individual requiring SCORE to implement IAVAs works for SPAWAR. In fact, the person complainant identified works for COMPACFLT and is the Information Assurance Manager in charge of COMPACFLT N643.

[5] As discussed later, we found the personnel who make changes to the SCORE network in response to IAVAs are actually SCORE employees.

discussions were not recorded or under oath. The investigator contacted every witness on the complainant's list, either for an informal discussion, or a formal interview. Appendix A identifies all individuals contacted.

15. On 23 January 2014, the investigator conducted a follow-up interview with the complainant to review the other evidence collected during the investigation, and to give the complainant an opportunity to comment on the proposed findings of the report. The complainant's remarks are described at the end of the findings of fact section (paragraphs 31-33 and 35, below).

16. FACSFAC and SCORE provided the following documents:

a. FACSFAC San Diego Instruction 3550.1D, Range User's Manual, 27 April 2012, with Changes.

b. Joint letter Commander, Naval Base Coronado/FACSFAC, Ground Range Standard Operating Procedures, 30 July 2013.

c. SCORE Network Discrepancy Log, excerpts. Note this was the result of a data query of a database SCORE maintains.

d. SCORE Discrepancy Reports 15 April 2013, 22 August 2013, and 26 September 2013. Note these were the result of a data query of a database SCORE maintains.

Summary of Allegations and Conclusions

17. We determined the following allegation was appropriate for investigation:

Allegation One: That COMPACFLT N6's means of conducting information assurance activities is causing regular disruption to command communications within another Navy component, SCORE, endangering the lives of service members and the general public.

18. We concluded that Allegation One is not substantiated because no other witness, record, or other evidence supported complainant's initial statement[6] that information assurance measures caused a safety hazard on SCORE-controlled exercise ranges. Moreover, when re-interviewed, complainant agreed the facts provided by the other witnesses generally were correct.

[6] See footnote 2 above.

Summary of Evidence Obtained During Investigation

Allegation One

That COMPACFLT N6's means of conducting information assurance activities is causing regular disruption to command communications within another Navy component, SCORE, endangering the lives of service members and the general public.

Findings

19. During the 1990s, SCORE created a computer network to control its instrumented exercise ranges. In the absence of an integrated network internal to DoD or DON such as the Navy-Marine Corps Intranet (NMCI), SCORE used a commercial internet service provider, AT&T. The SCORE network also predates the evolving DoD information assurance requirements that ensure the security of DoD computer networks such as NMCI, and information contained on those networks. Although the SCORE network has evolved over the years, SCORE uses this same commercial network to perform these functions today. Within DoD, the SCORE AT&T network is considered a "legacy system" that DoD and DON are working to replace with more secure systems.

20. Prior to 2010, regulations governing DoD computer networks authorized exemptions for DoD activities to operate computer networks outside of the NMCI. From the creation of the NMCI to 2010, DoD information assurance requirements have grown more stringent in response to various threats, and the security of DoD computer networks connected to commercial internet service providers have become a particular concern.

21. In July 2010, the Commanding Officer, FACSFAC and the Information Assurance Manager, COMPACFLT N643, discussed how to operate the SCORE computer network more securely and decided to move the SCORE network onto the NMCI. Although SCORE has progressed towards this goal, its computer network is still separate from NMCI, and NMCI personnel have no means of accessing it or making changes to it.

22. Only SCORE personnel have made changes to SCORE's computer network. TENTH Fleet and NCDOC, or their predecessors that performed their functions, required all Navy computer networks, including SCORE's, to reasonably comply with information assurance measures. COMPACFLT N643 worked with SCORE to make informed decisions about how to comply with information

assurance requirements necessary to address vulnerabilities, but only SCORE personnel have implemented IAVAs on its network or made other changes to the network.

23. Since before July 2010, SCORE has routinely monitored all air traffic in the exercise ranges under SCORE control. To accomplish this, SCORE employs three Range Safety Officers. One of them will be on duty whenever there are exercises planned with a significant impact on the air space surrounding the SCORE ranges. The Range Safety Officer's sole focus is to ensure air traffic, whether civilian or military, does not create any unsafe conditions for anyone in or around San Clemente Island.

24. Prior to August 2013, SCORE did not attempt to maintain communication with units conducting ground exercise on the in-shore and near-shore San Clemente Island ranges while these exercises were in progress. Prior to August 2013, SCORE ensured the safety of in-shore and near-shore exercises on San Clemente Island only through scheduling.

25. SCORE established a Range Coordination Center on 19 August 2013 in order to use the SCORE exercise ranges to conduct ground exercises more efficiently. The Range Coordination Center now maintains contact with the exercising units. The exercising unit will check into the exercise area with the Range Coordination Officer. The Range Coordination Officer will notify the exercising unit of any conditions affecting the exercise area, such as the presence of unexploded ordnance or sensitive species at particular locations. The Range Coordination Officer will monitor the exercise, and contact the unit if it is deviating from the planned exercise, or if there are any emerging safety hazards.

26. SCORE schedules maintenance periods for its computer network, and during these times it is unavailable. These periods last approximately one week, and occur two to four times per year. All witnesses except the complaint stated these periods are scheduled in advance and have no impact on exercises in SCORE-controlled ranges. The complainant did not explicitly state these week-long periods were unplanned, sudden losses of the SCORE computer network, but he implied that was the case by discussing all network outages, planned and unplanned, as if there was no distinction between scheduled system maintenance and unplanned outages.

27. The investigator asked the Range Safety Officers to identify and describe any unplanned outages or other occasions when they have lost the ability to communicate with exercise participants since 2010. One said he lost communication with a helicopter for approximately 90 seconds; he stated he was not aware of any other instance. The other two Range Safety Officers could not identify any specific instances of unplanned outages, but stated there might have been one or two outages of short duration per year. One Range Safety Officer said an outage could last as long as an hour; the other stated the longest unplanned outage he'd experienced was "seconds to minutes" in duration. Other witnesses who had second hand knowledge of communication difficulties provided similar descriptions, but with less detail. All Range Safety Officers and all other witnesses stated they could not attribute the outages to information assurance measures. All Range Safety Officers and all other witnesses stated "lost comms" safety procedures prevented these instances from causing a safety hazard on SCORE controlled ranges.

28. The investigator asked the Range Coordination Officers to identify and describe any instances when they lost the ability to communicate with exercise participants since 2010. They could identify none, and pointed out that the SCORE Range Coordination Center had no responsibility to maintain communication with on-shore and near-shore exercise participants before August 2013.

29. The Range Coordination Officers stated they have two communications channels. One relies on the SCORE computer network; the other is a short wave radio network (the Enterprise Land Mobile Radio System or "ELMRS"), which is completely separate from the SCORE computer network. They stated that they have had infrequent difficulties communicating with exercise participants on the SCORE computer network, perhaps one or two since the Range Coordination Center was established in August 2013. All Range Coordination Officers stated they could not attribute the outages to information assurance measures; one stated that exercise participants themselves are most often the source of these difficulties. All Range Coordination Officers stated that during these periods ELMRS was working properly and they were able to maintain communications. They also stated "lost comms" safety procedures provided further safeguards. All Range Coordination Officers stated the infrequent loss of the ability to communicate over the SCORE computer network did not cause a safety hazard on the SCORE controlled ranges because

they were of short duration and alternate means of communication are available.

30. The investigator reviewed with the computer network support personnel the documented incidents of information assurance measures causing technical problems with the SCORE computer network. The documents do not identify any instances of an information assurance measure causing an inability to communicate with exercise participants.

31. On 23 January 2014, the investigator conducted a follow-up interview with the complainant. He agreed that only SCORE personnel make changes to the SCORE computer network, based on direction from and with the advice of outside activities (e.g. TENTH Fleet, NCDOC and COMPACFLT N643).

32. The investigator discussed with the complainant degradation of computer network performance, which the complainant attributed to IA measures, and the occasional loss of some component(s) of the network. He clarified that in his original complaint he intended to describe any loss of function in the network, even those short of complete disruptions of both auditory and visual communications, and he also intended to include planned, scheduled maintenance periods when the network would be unavailable. If one counted only unanticipated, complete disruptions of both auditory and visual communications between range participants and Operations Center personnel, he agreed with the Range Safety Officers' descriptions of their frequency and duration. The complainant stated that a loss of function short of a complete disruption of both auditory and visual communications is not a safety issue, but he also pointed out that the inability to continue with an exercise can still be a significant operational issue. Other witnesses in prior interviews also stated that a loss of function causing an exercise to be cancelled or rescheduled is a significant operational issue but, as noted in paragraph 27, such unplanned outages are rare and of short duration.

33. The investigator discussed with the complainant the establishment of the Range Coordination Center for on-and-near-shore exercises. The complainant agreed that it began operations in August 2013. He acknowledged the primary communication channel for on-and-near-shore exercises is ELMRS, which is independent of the SCORE computer network, and that SCORE has extensive "lost communications" standard operating procedures to avoid safety hazards. Therefore, computer network

problems were unlikely to cause communication issues for on-and-near-shore exercises. The complainant stated that starting in 2010, he and other individuals voiced their concerns about safety on SCORE controlled ranges, and that the Range Coordination Center was a response to those concerns. This differs slightly from how other witnesses described the decision to establish the Range Coordination Center, but the complainant's and the other witnesses' accounts are consistent.

34. All witnesses other than the complainant stated that the SCORE computer network is generally reliable. Two witnesses who had worked at FACSFAC San Diego or another military exercise range said SCORE's computer network was more reliable than the network at their prior commands. All witnesses stated there was the occasional problem with the SCORE computer network and the SCORE network has perceptibly slowed since 2010, but these problems did not interfere with their ability to do their jobs.

35. In his 23 January 2014 follow-up interview, the complainant stated that the SCORE computer network's reliability has significantly improved since November 2013, and since the establishment of the Range Coordination Center, his safety concerns have been adequately addressed.

Discussion and Analysis

36. The OSC tasking letter is based on the premise that in carrying out their cyber security mission, information assurance personnel not assigned to SCORE force connections of the internal SCORE wiring to unsuitable circuits controlled by the NMCI. We found no evidence that would support this contention. On the contrary, the SCORE computer network is not connected to the NMCI. Moreover, only SCORE personnel have installed IAVAs or made changes to the SCORE computer network. When asked for a clarification, the complainant agreed only SCORE personnel make changes to the SCORE network.

37. The OSC tasking letter states that information assurance measures disrupt both auditory and visual communication between range participants and Operations Center personnel and asserts these communications blackouts occur at least once a day and vary in length from one hour to as long as two weeks. No witness described unplanned outages of such frequency or duration. In fact, witness testimony establishes that only regularly scheduled outages, which occur two to four times per year and last, on about one week, approach the duration

mentioned in the tasking letter. When re-interviewed, the complainant clarified that when he first contacted OSC, he intended to report any loss of function in the SCORE computer network and to report all periods when the SCORE computer network was unavailable, including those due to scheduled maintenance. The complainant agreed with the witnesses' descriptions of unanticipated, complete disruptions of both auditory and visual communications between range participants and Operations Center personnel. Moreover, there was not one instance of a communication outage that could be attributed to information assurance measures. The investigator ensured he contacted every person the complainant recommended he speak to and interviewed all who indicated they had knowledge of the matters raised in the tasker. All of the witnesses stated the SCORE computer network was reliable and the difficulties they did experience did not prevent them from doing their jobs.

38. The OSC tasker also stated the loss of communication with exercise participants has created a substantial and specific threat to both Navy personnel participating in fleet exercises in the SCORE range and members of the general public traveling in the vicinity of the range. The witnesses stated that there are infrequently difficulties communicating with exercise participants, although none could be attributed to information assurance measures. SCORE employs redundant communication channels and has in place "lost communications" procedures for these situations. This ensures that SCORE maintains the ability to conduct exercises safely on its ranges. The complainant agreed that since the establishment of the Range Coordination Center and the recent improvement in the reliability of the SCORE computer network, his safety concerns have been adequately addressed.

Conclusion

39. The allegation that COMPACFLT N6's means of conducting information assurance activities is causing regular disruption to command communications within another Navy component, SCORE, endangering the lives of service members and the general public is NOT SUBSTANTIATED.

Actions Planned or Taken

40. None.

Personnel Actions Taken

41. None.

Appendix A - Witness List

The following individuals provided formal, recorded interviews under oath. Some of these individuals also provided background information outside of the formal interview or pertinent documents.

1. Range Technical Support Manager, SCORE, 8 November 2013.

2. Commanding Officer, FACSFAC, 7 November 2013.

3. Officer in Charge, SCORE, 7 November 2013.

4. Assistant Officer in Charge and Range Safety Officer, SCORE, 7 November 2013.

5. Information Assurance Officer, SCORE Contractor Employee, 8 November 2013.

6. Director of Operations, SCORE, 6 November 2013.

7. Mr. David Richardson, Technical Director, SCORE, 3 October and 5 November 2013 (complainant).

8. Information Assurance Manager (N643), COMPACFLT, 12 November 2013.

9. Range Manager and Ground Activities Range Coordination Officer, SCORE, 7 November 2013.

The following individuals provided information informally. They did not participate in formal interviews.

1. Range Scheduler and Exercise Coordinator, SCORE

2. Range Safety Officer, SCORE

3. Computer Systems and Budget Analyst, SCORE

4. Information Assurance Manager, SCORE

5. Network Support Engineer, SCORE

6. Range Safety Officer, SCORE

7. Range Scheduler and Exercise Coordinator, SCORE

8. Program Manager, SCORE

9. Network Support Engineer, SCORE Contractor Employee

10. Network Support Engineer, SCORE

11. Office Manager, SCORE

12. Ground Activities Range Control Officer, SCORE

13. Program Manager, SCORE

14. Program Manager, SCORE

15. Computer Engineer, Naval Undersea Warfare Center

16. Network Support Engineer, SCORE Contractor Employee

17. San Clemente Island Range Manager and Range Coordination Officer, SCORE

18. Range Scheduler and Exercise Coordinator, SCORE