



Office of the Washington State Auditor
Pat McCarthy

Whistleblower Investigation Report

Department of Fish and Wildlife

Published March 1, 2018

Report No. 1020871





**Office of the Washington State Auditor
Pat McCarthy**

March 1, 2018

Joe Stohr, Acting Director
Department of Fish and Wildlife

Report on Whistleblower Investigation

Attached is the official report on Whistleblower Case No. 17-035 at the Department of Fish and Wildlife.

The State Auditor's Office received an assertion of improper governmental activity at the Department. This assertion was submitted to us under the provisions of Chapter 42.40 of the Revised Code of Washington, the Whistleblower Act. We have investigated the assertion independently and objectively through interviews and by reviewing relevant documents. This report contains the result of our investigation.

If you are a member of the media and have questions about this report, please contact Assistant Director for Communications Kathleen Cooper at (360) 902-0470. Otherwise, please contact Whistleblower Manager Jim Brownell at (360) 725-5352.

Sincerely,

Pat McCarthy
State Auditor
Olympia, WA

cc: Governor Jay Inslee
Mario Cruz, Internal Auditor
Kate Reynolds, Executive Director, Executive Ethics Board
Jennifer Wirawan, Investigator

WHISTLEBLOWER INVESTIGATION REPORT

Assertion and Results

Our Office received a whistleblower complaint asserting a Department of Fish and Wildlife (Department) employee (subject) grossly mismanaged his responsibilities by misrepresenting information to the federal government.

We found no reasonable cause to believe an improper governmental action occurred.

About the Investigation

The Bonneville Power Administration (BPA) is a federal agency that provides grants to fund regional efforts to protect and rebuild fish and wildlife populations. The Department receives more than 20 grants each year worth approximately \$15 million.

As part of the grant process, BPA requires the Department attest to its compliance with data security standards. Historically, the Department's Chief Information Officer (CIO) has signed the annual attestation. By signing the attestation, the signer certifies that all of the programs within the Department that receive the grants comply with security standards.

On July 18, 2016, an information technology employee sent the CIO an email requesting he sign the attestation. The CIO wrote that, based on a preliminary internal audit, he believed the program was not compliant with required security standards. The employee responded the attestation is a formality that assures the Department "will protect" data.

In a July 27, 2016, meeting, the CIO and the Chief Information Security Officer (CISO) informed the subject, who works for the Department's fish program, that neither would sign the attestation. According to meeting minutes and witness interviews, the CIO and CISO told the subject the program was not compliant with required security standards and they needed more time to review the system to ensure compliance. One witness told our Office the CIO was concerned that signing the document would be "dishonest" and the subject said he was willing to take a risk because the program needed the money. The subject said he signed the document after the meeting.

During an interview, the subject said he knew the CIO was unwilling to sign the attestation, but he had to do something: "\$15 million and state jobs were at risk." He said he asked questions regarding the data, the attestation and Department policy and based on the responses, he believed he did his due diligence before he signed.

The subject said the IT employee told him that the BPA viewed the attestation as a "formality" and that he did not believe the fish program was non-compliant. When asked why he trusted the opinion of the IT employee over that of the CIO and CISO, he said he trusted him because he was extremely knowledgeable. However, he said he did not base his decision solely on the

information he received from the employee. He said the CIO's reasons not to sign the attestation were unreasonable and if he had received a valid reason, he would not have signed.

We spoke with BPA's CISO, who said that the attestation was "almost" a formality and was meant to ensure there are "reasonable precautions in place" to protect BPA data. He said the data in question is publicly available, and if the risk were greater, they would require an audit. He said the lack of compliance "would not prevent the BPA from going forward with the grant." He said BPA no longer requires the attestation.

"'Gross mismanagement' means the exercise of management responsibilities in a manner grossly deviating from the standard of care or competence that a reasonable person would observe in the same situation."

"Improper governmental action" is defined as "any action by an employee undertaken in the performance of the employee's official duties [...] which is in violation of federal or state law or rule, if the violation is not merely technical or of a minimum nature."

We found the subject did sign the attestation, which may have misrepresented information to the federal government; however, the BPA representative said the risk to the region and the mission is much greater if the grant is not issued. The subject's actions were minimal in nature and do not rise to the level of gross mismanagement. Therefore, we found no reasonable cause to believe an improper governmental action occurred.

State Auditor's Office Concluding Remarks

We thank Department officials and personnel for their assistance and cooperation during the investigation.

WHISTLEBLOWER INVESTIGATION CRITERIA

We came to our determination in this investigation by evaluating the facts against the criteria below:

42.40.020 Definitions

As used in this chapter, the terms defined in this section shall have the meanings indicated unless the context clearly requires otherwise.

- (4) "Gross mismanagement" means the exercise of management responsibilities in a manner grossly deviating from the standard of care or competence that a reasonable person would observe in the same situation