

American Federation of Government Employees  
National Council of HUD Locals 222


*Affiliated with AFL-CIO*

451 7th Street, SW, Suite 3172  
Washington, DC 20410

Holly Salamido, President  
E-mail: Holly.Salamido@hud.gov

Phone: 202-402-5243  
Fax: 202-708-7638

July 16, 2015

MEMORANDUM FOR: Michael Stein, Acting Director,  
Employee & Labor Relations Division 

FROM: Holly Salamido, President, Council 222 of HUD Locals

SUBJECT: Additional Proposals: HUD's response to the security breach of HUD bargaining unit employees' Personally Identifiable information (PII) through the U.S. Office of Personnel Management (OPM) cybersecurity incident

Pursuant to Article 5 of the HUD-AFGE Council 222 Agreement, AFGE National Council of HUD Locals No. 222 (Council or AFGE Council 222) submits additional proposals regarding the Department's response to the security breach of HUD bargaining-unit employees' Personally Identifiable information (PII) through the U.S. Office of Personnel Management (OPM) cybersecurity incident affecting its systems and data that may have exposed the personal information of current and former HUD Bargaining unit employees.

The below proposals supplement the Demand to Bargain submitted by the Council on June 5, 2015. These are preliminary bargaining proposals and are not to be considered all of the proposals that the Union will submit.

10. Statement of Purpose: These proposals are being furnished in the early stages of the Union's discovery of the OPM data breach. These are initial proposals that allow for a baseline response from the Agency immediately. The Union expects the Agency to respond with appropriate good faith and urgency to provide all possible protections as a result of this OPM lapse and government created crisis. The Agency should expect the Union to offer additional proposals and modifications of these proposals as the situation develops; the Union is not waiving its right to supplement, amend or withdraw its proposals throughout the duration of this crisis.

11. The Impact Letter: The Agency will send a letter ("Impact Letter"), within seven (7) calendar days of the execution of this Agreement, to each bargaining unit employee stating with full particularity:

- a. when the Agency learned of that employees data breach;
- b. when the Agency believes the breach occurred; and

- c. any and all employee information that could have been potentially compromised in the breach

The Agency will provide a hardcopy of the Impact Letter to the employee at the workplace and obtain a signed letter from the employee for receipt of acknowledgement. If the Agency is unable to furnish the Impact Letter to the employee within seven (7) calendar days of the execution of this Agreement, they will immediately send a copy of the Impact Letter to the employee's last known home address via registered mail or certified mail.

12. Identity Theft Training: The Agency will provide an employee training with identity theft protection experts ("Identity Theft Training") within thirty (30) calendar days of the execution of this Agreement, to each bargaining unit employee. The training will be, at a minimum, two (2) hours in length, and will cover, at a minimum, the following topics:

- a. how and when to lock, flag, or freeze credit reports;
- b. how and when to place a fraud alert or credit freeze on reports;
- c. how and when to renew or update alerts or freezes automatically;
- d. how and when to establish fraud alerts;
- e. how and when to notify banks, and credit card companies of a potential breach; and
- f. How and when to establish new accounts following with banks, and credit card companies.

The training will be conducted on administrative time, allocated for the purpose of this meeting.

13. Financial Security Specialist: The Agency will provide employees notice, both electronic and hard copy, offering Agency funded Financial Security Specialist consultations, within thirty (30) calendar days of the execution of this Agreement, to each bargaining unit employee. The Agency will offer employees two (2) hours of time to review the employee's financial situation, the potential threats to their financial well-being due to the breach, and recommended or necessary courses of action, either:

- a. with a financial security specialist paid for and provided by the Agency; or
- b. with a financial security specialist selected by the employee, reimbursed by the agency within one (1) pay cycle of the submission of proof of payment. The consultation will be conducted on administrative time, allocated for the purpose of this meeting.

14. Lifetime Credit Monitoring: The Agency will provide bargaining unit employees with lifetime credit monitoring by a company of the employee's choosing, selected from among 5 choices provided and paid for, in its entirety, by the agency.

15. Necessary Administrative Time

For the first sixty (60) calendar days following the execution of this Agreement, the Agency will provide to each bargaining unit employee a block of twenty four (24) hours of administrative time to assess their exposure, monitor credit ratings and credit card and bank accounts, and make necessary account changes to protect the employee's assets and credit, including but not limited to changing account information for credit cards and bank accounts.

After the first sixty (60) calendar days following the execution of this Agreement, bargaining unit employees will be provided two (2) hours of administrative time per month to continue to monitor their credit to prevent abuse. If additional time is needed to deal with particular problems flowing from the breach, the Agency will grant a reasonable amount of additional administrative time. In such cases, the Agency may require supporting documentation before granting additional time. The Agency will return the supporting documentation to the requesting employee after review, to avoid the loss of additional potentially sensitive employee information.

16. Use of Agency Equipment: The Agency will provide bargaining unit employees use of government equipment, (including but not limited to computers, telephones, fax machines, scanners, photocopiers) to coordinate with financial institutions, credit card companies and banks, credit rating agencies, other government agencies and other organizations as needed to secure the employee's financial well-being. The need of the employees to use government equipment is an ongoing need, and is expected to continue for employee's career with the Agency.

17. Ongoing Briefings and Employee Updates: The Agency will provide bi-weekly briefings, either in person, by telephone or video teleconference, to the Union regarding developments regarding the data breach. These briefings will not, standing alone, satisfy the Agency's notice requirements relating to bargaining obligations. The Agency will provide updates to the bargaining unit employees no less frequently than once per-month, and will provide all information to the Union no less than one (1) full workday in advance.

18. Make Whole: The Agency will make all bargaining unit employees whole for any and all expenses and losses incurred as a direct or proximate result from OPM data breach.

19. Credit Ratings and Security Clearance: The Agency will provide any and all necessary training or assistance for bargaining unit employees impacted by the data breach to maintain credit ratings required to maintain or acquire work related security clearances.

If there are any other questions or concerns, please contact me at (202) 402-5243.