MEMORANDUM OF UNDERSTANDING
between
National Archives and Records Administration
and
American Federation of Government Employees
Council 260

Pursuant to negotiations between the above parties regarding the 2015 OPM data breach and its impact on bargaining unit employees, and in the spirit of cooperative labor relations, the parties agreed to the following:

1) NARA Management will allow employees to use work time to register for credit monitoring and fraud protection services with the OPM security contractor, CSID, and to comply with other OPM and NARA direction or guidance related to the breach (e.g. changing eOPF passwords, monitoring credit ratings and accounts). FRCP employees will be provided with a non-production task code for such time.

2) Management will grant a reasonable amount of administrative leave to allow employees to address other consequences of the data breach. Administrative leave will be granted at the discretion of the employee's supervisor and on a case-by-case basis. Reasonable requests will not be denied absent a compelling need. Denials of administrative leave for purposes related to the data breach or identity theft may be grieved through the negotiated grievance procedure.

3) Management will permit an employee who has a regular or ad-hoc telework agreement to use the work time under paragraph (1) and/or approved administrative leave that is available under paragraph (2) while teleworking.

4) Management will provide employees with space and allow use of equipment such as photocopiers and fax machines. Management will allow employees to make telephone and other communications with the necessary privacy. The need to use government equipment for this purpose is an ongoing need.

5) Within a reasonable amount of time, Management will provide employees with resources (including training) that:

   (a) Clearly describe how to comply with OPM and NARA direction and guidance for mitigating the breach, and accessing on-line resources in particular;

   (b) Identify specific actions to take in order to mitigate the risk of identity theft and actions to take if an actual incident of identity theft is suspected or occurs; and

   (c) Describe the relationship between credit ratings and suitability for a work-related security clearance and the actual or potential consequences of the subject data breach on an employee's ability to obtain or maintain a security clearance.

6) Both parties mutually agree to reconsider the terms of this agreement as needed, but no later than six months before the first expiration date of any of the Government-sponsored credit monitoring services or identity theft insurance offered as a result of the subject data breach.

7) The Agency will give regular updates to employees and union officials whenever there are substantive new developments regarding the data breach and its impact on employees.

8) Upon signatures of the parties listed below, this MOU will be effective.

7/21/15 21 July 2015

ASHBY CROWDER DATE DAVID FERRIERO DATE

Executive Vice President, AFGE Council 260 Archivist of the United States