**OPM Data Breach**

**This notice applies to current and former midshipmen and active/retired alumni.**

**Background**

The Office of Personnel Management (OPM) has recently announced two separate but related cyber security breaches. If you have applied for or been granted a security clearance since 2000, you could be affected. The breach affects current and prior federal employees (and their spouses/co-habitants) who have undergone a background check and filled out an SF85 or SF86 after the year 2000. Individuals who underwent background investigations prior to 2000 may have been affected but it is unlikely. The breach includes personal information including, but not limited to, name, Social Security numbers, dates of birth, educational history, travel history, financial history and court records.

**Notification Timeline**

-In June 2015, OPM began sending out notifications about the first data breach

-Notifications for the second breach will be released starting in late September 2015 and continuing for several weeks.

-Notifications will be sent to the individuals work email address from the email OPMcio@csid.com (you may need to check your spam folder)

-If OPM is unable to contact the individual via email, a postal notification will be sent

-OPM will continue to notify the individual until the PIN is activated.

**If Notified**

-Go to <https://opm.csid.com/pin>to access the CSID website

-Enter Unique PIN from notification

-Sign up for 18 months of complementary credit monitoring and identity theft insurance up to 1 million dollars. Registration is online only.

-Regardless of whether or not an individual registers with CSID, they will have credit monitoring and identity theft insurance until December 7, 2016.

-Within 24-72 hours you will receive a CSID identity protection report that shows if any of your personal accounts have been used by persons other than yourself

-Go to [www.transunion.com/fraud](http://www.transunion.com/fraud) to sign up for fraud alerts. This will have creditors notify you before new accounts are opened under your name.

**Additional Steps**

-Change passwords on all of your accounts frequently. This includes online banking, email and social media sites.

-Actively monitor all personal accounts for abnormal activity. -Within 24-72 hours you will receive a CSID identity protection report that shows if any of your personal accounts have been used by persons other than yourself

-Get yearly free credit reports from [www.annualcreditreport.com](http://www.annualcreditreport.com)

-If you think you are the victim of identity theft, go to [www.identitytheft.gov](http://www.identitytheft.gov)

-Do not open emails from suspicious senders or click on embedded links

-Do not give out personal information over the phone or internet unless you are positive about the recipient’s validity.

-Persons with USAA banking can sign up for credit monitoring for $5.50/month whether or not they were affected by the data breach.

**Resources**

OPM Website <https://www.opm.gov/cybersecurity>

Extended Date Breach Portal <http://www.secnav.navy.mil/OPMBreachDON/Pages/faqs.aspx>

General Identity Protection - <http://www.secnav.navy.mil/OPMBreachDON/Pages/toolkit.aspx#Employees>

Further Questions should be directed to LT Throckmorton at [vthrock@umich.edu](vthrock%40umich.edu)