WWW.MARFORRES.MARINES.MIL

MARINEFORCESRESERVE | AUGUST 2015

COMMUNICATOR

BY THE NUMBERS

* As of July 2015

Total Marine Corps Reserve
109,558

Individual Ready Reserve
70,403

Selected Marine Corps Reserve
30,946

Active Reserve
2,252

Trainees
3,327

Individual Mobilization Augmentees
2,630

Total SelRes
39,155

Active Component End Strength
187,280

U.S. Navy End Strength
1,581

Exercises
76

Operations
116

Total Deployed
192

Authorized End Strength
39,600

RESERVE SITES

Tenant Locations
134

Owned Sites
27

Family Housing Sites
3

LT. GEN. RICHARD P. MILLS

Commander, Marine Forces Reserve

It has been widely reported that the Office of Personnel Management recently discovered two separate hacking incidents in which sensitive personal information was stolen. The first incident involved the breach of information of an estimated 4.2 million current and former federal employees. In the second incident, more than 21.5 million individuals had information compromised that included up to 19.7 million individuals who applied for background investigations and 1.8 million others, including spouses and dependents of the applicants.

We do not yet know the full scope of the damage – including numbers of Marines and Sailors of MARFORRES; but if you have applied for a security clearance since 2000, it may be you.

Cyber threats are nothing new. Identity theft and the vulnerability of our personal information remains very real. The most recent data hacks have exposed some critical vulnerabilities and may embolden future hackers. We must deal decisively with this threat as we do with any other enemy. I expect all Marines and Sailors of MARFORRES to be proactive in protecting yourselves from these threats. Use the following information to make yourselves a hard target, and keep your heads on a swivel. Semper Fidelis.

Click on the names below to view the bios and photos

LEADERSHIP

Secretary of the Navy	Hon. Ray Mabus	Sergeant Major, Marine Forces Reserve	Sgt. Maj. Anthony A. Spadaro
Commandant of the Marine Corps	Gen. Joseph F. Dunford, Jr.	Command Master Chief, Marine Forces Reserve	CMDMC Chris Kotz
Assistant Commandant	Gen. John M. Paxton Jr.	4th Marine Division	Maj. Gen. Paul W. Brier
Sergeant Major of the Marine Corps	Sgt. Maj. Ronald L. Green	4th Marine Aircraft Wing	Maj. Gen. William T. Collins
Commander, Marine Forces Reserve	Lt. Gen. Richard P. Mills	4th Marine Logistics Group	Brig. Gen. Patrick J. Hermesmann
Executive Director, Marine Forces Reserve	Mr. Gregg T. Habel	Force Headquarters Group	Brig. Gen. Helen G. Pratt

OPM Security Breach

What happened and what you can do.

What happened: The Office of Personnel Management discovered two separate cyber-security incidents that affected the data of members of the military, federal employees, contractors and others.

Data Breach	What was stolen	Notification
April 2015	• Personnel records of 4.2 million current and former federal employees, including members of the military. • Included records such as full names, birth dates, home addresses and Social Security numbers.	Notification continues via U.S. mail and email from OPMcio@csid.com
June 2015	• Background investigation records of current, former and prospective federal employees, including members of the military and their dependents. • Included 21.5 million Social Security numbers as well as all other data that goes into the application for security clearance. • OPM estimates that if you applied for a security clearance after the year 2000, you were "most likely affected."	Notification will be in the same manner.

General

- Don't answer unsolicited calls and emails or provide personal information to anyone asking about federal employees or other internal information.
- Don't reveal personal, financial or other sensitive information in emails.
- Don't follow links sent from an email address you are unfamiliar with.
- Install and use anti-virus software, firewalls and email filters.
- Monitor all checking and other financial accounts, and immediately report any suspicious activity.
- Consider placing a fraud alert on your credit file so creditors will contact you before a new account is opened in your name.
- Request a free credit report to see if any new accounts or credit inquiries show up.

If you suspect identity theft, do the following:

1. Contact Equifax, Experian, and TransUnion to report your identity has been stolen.
2. File a police report.
3. Contact each company where you think you might have been a victim, and file a complaint.
4. Keep records of all conversations and activities.
5. File a complaint with the Federal Trade Commission.
6. If you suspect your SSN has been stolen, contact the Social Security Administration.
7. If you suspect improper use of your tax records, contact the Internal Revenue Service.

Helpful Links:

- Central information hubs on the OPM data breaches
- Resources on identity theft, including warning signs and what to do if your identity has been compromised
- Resources that define phishing and how to report phishing attempts
- Helpful steps to ensure your computer is as safe as possible
- Department of Navy Cybersecurity Tookit