[COMPANY]
LETTERHEAD]

[DATE]

[Name]
[Address 1]
[Address 2]
[City], [State] [Zip]

Dear [**Name**],

On April 27, 2017, Bechtel Oil, Gas & Chemicals Construction Services, Inc. ("Bechtel") discovered a data incident which may have resulted in unauthorized access or acquisition of your personal information as the result of an inadvertent email sent to other Bechtel email addresses. The incident occurred on April 27, 2017. The data elements involved may have included name, addresses, telephone number, Social Security number, and date of birth. At this time, we are not aware of, and do not anticipate, any improper use of the information contained in the email. Nevertheless, in an abundance of caution, we are providing this notice to inform you of the incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. We apologize for any inconvenience this may cause you and assure you we are working diligently to resolve this incident.

Immediately upon discovering the incident, we commenced an investigation to determine its scope and identify those affected. We worked with our assembled internal response team including our IS&T department and took steps to secure our information systems. These efforts included the IS&T department recalling the email message and removing the email and its contents from all email accounts which received the email. Additionally, we confirmed in writing with each recipient of the email that the email and its contents had been deleted and no copies printed or otherwise retained. Set forth below are additional steps you can take to protect your identity and personal information.

We treat all personal information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. Theft of data and similar incidents are difficult to prevent in all instances, however, we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again.

If you have questions or concerns you should call **[INSERT CONTACT TELEPHONE NUMBER].** Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

[INSERT NAME]
[INSERT TITLE]

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:

- Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a 90 day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert

tab, visit www.fraudalerts.equifax.com or call the auto fraud line at 1-877-478-7625, and follow the simple prompts. This fraud alert will remain on your credit file for 90 days.

- Place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies. Credit reporting agencies charge a $5 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include (documentation for both the spouse and the victim must be submitted when requesting for the spouse's credit report) (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth; (iii) if you have moved in the past 5 years, the addresses where you have lived over the prior 5 years; (iv) proof of current address such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable (vi) payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.transunion.com

2. Contacting the Federal Trade Commission ("FTC") either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

3. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

4. If you believe you are a victim of identity theft you should immediately report same to law enforcement and/or your state attorney general.

5. This communication was not delayed at the request of law enforcement.

6. *For Maryland Residents*: The contact information for the Maryland Office of the Attorney General is: Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; Telephone: (888) 743-0023; website: http://www.oag.state.md.us.

7. *For North Carolina Residents*: The contact information for the North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: www.ncdoj.com/.