

# Protecting What Is Ours - What's Next



PRESENTED BY

**Sylvia M. Chavez**  
Security Awareness Coordinator

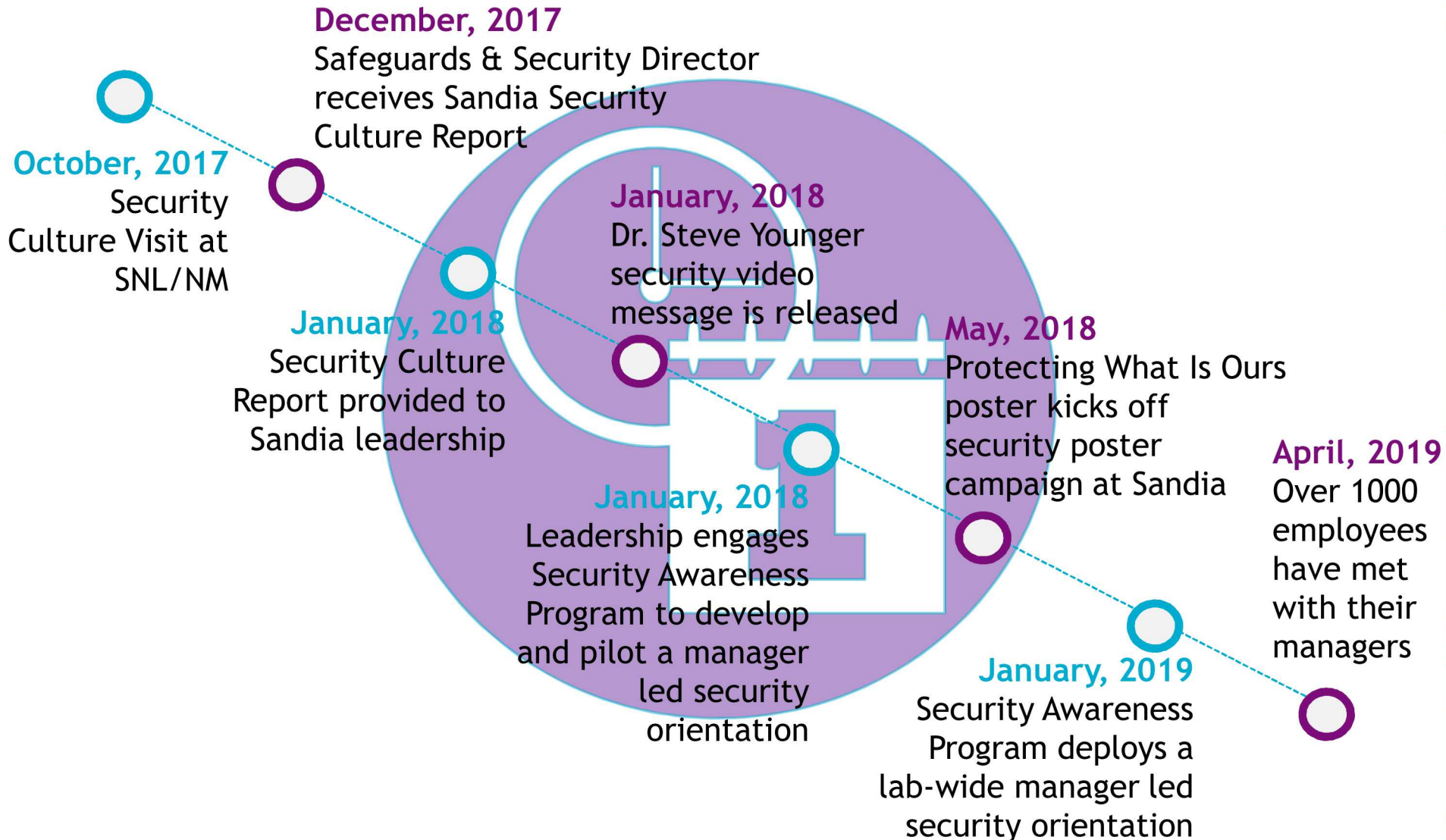


SAND2019



Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

# What Happened?



# Culture Results are Motivators

Dr. Younger Security video motivated Safeguards and Security to initiate additional efforts to raise security awareness and change the culture.



**Steve Younger**  
Laboratories Director

*Delivers a message  
of **personal  
responsibility**  
for security.*



# Culture Results are Drivers

## Protecting What is Ours Poster

kickstarted a campaign to establish a relationship between leadership and all Members of the Workforce.

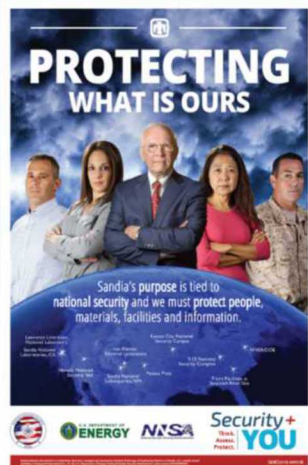


## Posters

at all sites provides trusted data to the line that to encourage a partnership with security to do better security.



**Security Culture Report** identified issues that Safeguards and Security already knew and garnered support for additional awareness activities.



# Culture Results Leads to New Ideas

*Security Awareness  
deploys a lab-wide  
manager led program  
specific security  
orientation.*



## SEC175

### Clearance Holder Program Orientation

2018-03-09 v6

Individual's Name: \_\_\_\_\_ Org: \_\_\_\_\_ ☐ Employee ☐ Contractor ☐ Student  
(Please Print)

CLEARANCE: ☐ Q ☐ L ☐ \*Interim Q Clearance ☐ \*Temporary Security Clearance Upgrade (L->Q) ☐

\* Different limitations apply to Interim & TSCJ clearances (e.g., TS, SIGMA, SC, SAP, COMSEC, CRYPTO, NATO, US/UK MDA, etc.)

Managers: discuss the following items with the newly cleared or transferred employee or staff-augmentation contractor prior to allowing access to classified information or activities. Indicate completion by checking each box.

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Your Derivative Classifier (<a href="#">Link</a>)</li> <li><input type="checkbox"/> Your Classified Administrative Specialist</li> <li><input type="checkbox"/> Your Cyber Security Representative (<a href="#">Link</a>)</li> <li><input type="checkbox"/> Your Security Professional (<a href="#">Link</a>)</li> <li><input type="checkbox"/> PRINT and discuss the following resource materials:               <ul style="list-style-type: none"> <li>o <a href="#">Everything You Need to Know About Classified</a></li> <li>o <a href="#">Unclassified Controlled Information</a></li> <li>o <a href="#">Human Performance Indicators</a></li> </ul> </li> <li><input type="checkbox"/> Program-specific guidance related to information:               <ul style="list-style-type: none"> <li>o Potentially <a href="#">classified subject areas</a> (PCSAs)</li> <li>o High-risk program areas (e.g., SIGMA, SC, SAP)</li> </ul> </li> <li><input type="checkbox"/> Safeguards &amp; Security risks associated with your work area(s) and activities:               <ul style="list-style-type: none"> <li>o Unauthorized network transmissions</li> <li>o Not using R&amp;A or DC review</li> <li>o Classified associations/compilation (e.g., email chains)</li> <li>o Improper escorting/vouching</li> <li>o Other: _____</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li><input type="checkbox"/> If there is use of a Classified Network, review:               <ul style="list-style-type: none"> <li>o Handling/protecting passwords</li> <li>o Locking machines</li> <li>o KVM use. Be aware of the network you are working on.</li> <li>o Downshift. Do not assume information is unclassified.</li> </ul> </li> <li><input type="checkbox"/> Discuss past 3 years of center security incidents and lessons learned (reminder: details may be classified)</li> <li><input type="checkbox"/> Review applicable training:               <ul style="list-style-type: none"> <li>o SEC301 Classified Matter Training</li> <li>o SEC303 Classified Marking Training</li> <li>o SEC326A/B/C EDC &amp; Derivative Classifier Training</li> <li>o SEC180 Vault Type Room</li> <li>o Classified Subject Matter Briefing (<a href="#">Course Catalog</a>)</li> <li>o Other: _____</li> <li>o Other: _____</li> </ul> </li> <li><input type="checkbox"/> Other discussions, considerations, questions:               <ul style="list-style-type: none"> <li>o _____</li> <li>o _____</li> <li>o _____</li> <li>o _____</li> </ul> </li> </ul> |
|--|---|

Employee/Staff-Aug Contractor Printed Name	Signature	Date
Manager Printed Name	Signature	Date
Security Professional (if present) Printed Name	Signature	Date

Employee/Staff-Aug Contractor:

Retain the completed SEC175 checklist, and provide a copy to the training coordinator for entry into TEO.



Sandia National Laboratories is a multi-program laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2018-13942 TR



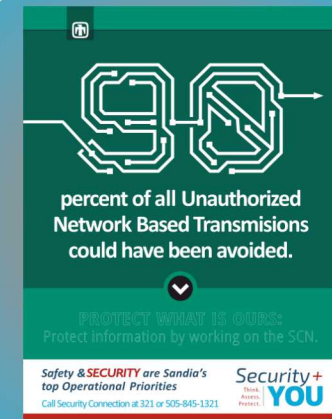
Security Connection  
805-845-1321  
security@sandia.gov

# What's Next

*Update Escorting policy to include use of U & E cards*



**Security+**  
Think. Assess. Protect. | **YOU**



*New **Gen-16**  
Awareness Activity*

*New posters for 2019 to  
identify incident trends*



*Security* +  
Think.  
Assess.  
Protect. | **YOU**