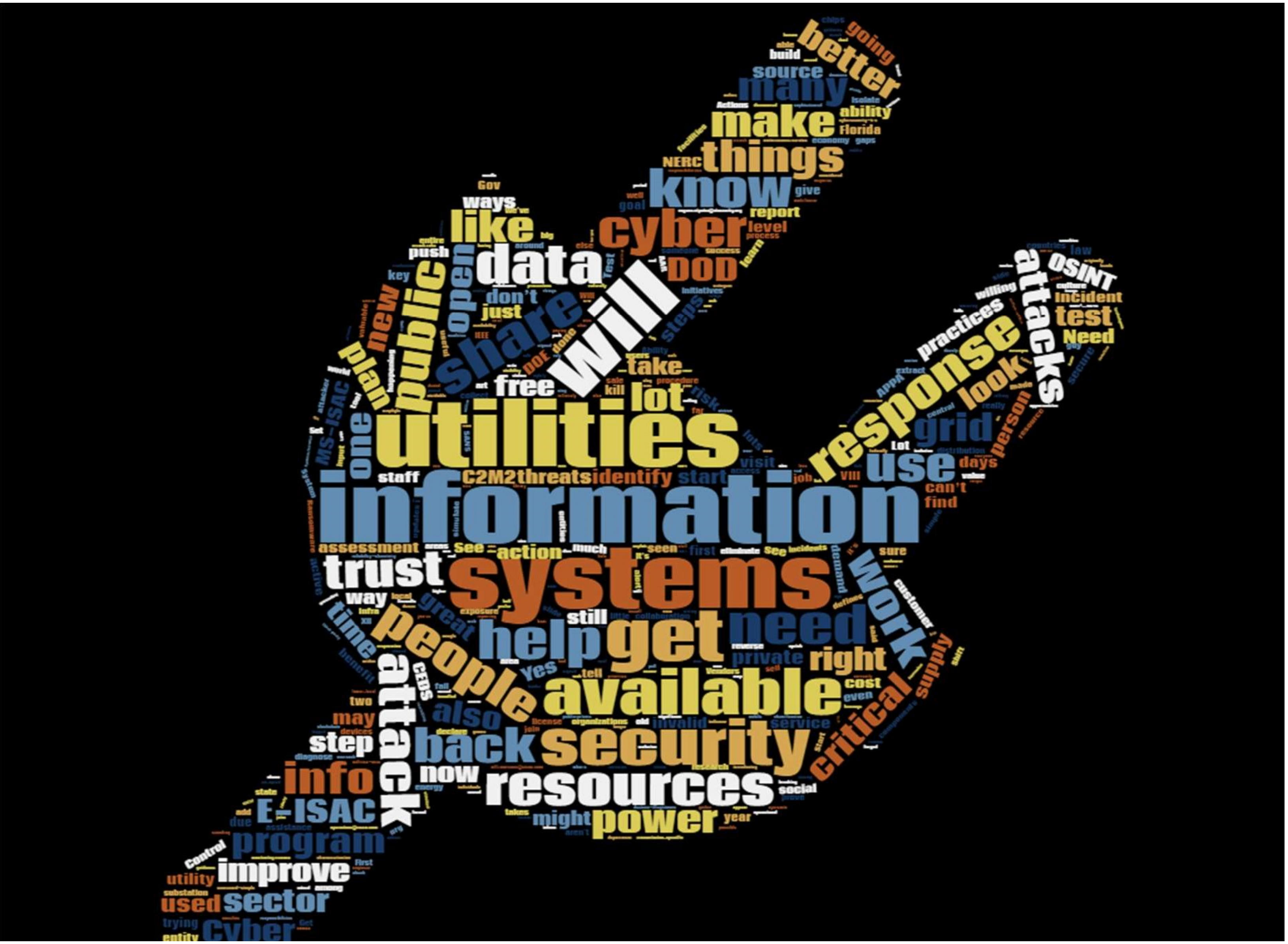
Day 1 – Actions We'll Take When We Get Back

- Develop/review/practice an incident response plan/playbook (12)
- Make better use of available free tools and resources, including training (11)
- Complete the Scorecard (8)
- Expand information sharing capabilities—explore new tools and expand resources (7)
- Test and perform backup restorations (5)
- Follow-up on Scorecard results (4)
- Connect with management and get buy-in regarding cybersecurity (4)
- Continue networking with peers, experts, ISACS—build trust circles (4)
- Identify "normal" baseline for systems—obtain a "golden copy" of your systems (3)
- Promote training—encourage staff to pursue and complete training (3)
- Take a risk-based and project-based approach to cybersecurity improvement (2)
- Email cybersecurity@publipower.org (1)

Day 1 – Reflections

- Take-aways:
  - Networking is valuable—between utilities, with ISACs, with APPA, with government
  - Connect with management
  - Develop awareness to know when there is a change in your network
  - Skill development, like cybersecurity, requires organization-wide culture/investment
  - The rooms are too dang cold


information
systems
utilities
will
security
available
resources
get
need
people
attack
response
help
share
data
trust
public
cyber
know
things
make
many
better
attacks
work
back
power
program
improve
sector
info
E-ISAC
critical
right
use
grid
look
lot
free
plan
open
new
like
one
time
also
now
step
may
great
identify
threats
C2M2
DOD
OSINT
test
incident
Need
practices
going
source
ability
Florida
NERC
report
level
ways
push
key
take
staff
start
assessment
action
still
private
cost
supply
person
days
find
used
utility
Cyber


control
power
Stage
going
things
make
room
sharing
new
report
incident
exercise
needed
Need
home
Cyber
great
attack
vendors
system
people
time
public
resources
available
security
know
look
also
Find
team
start
review
membership
ability
still
systems
better
plan
like
data
developed
test
utilities
sector
trust
need
looking
relationships
every
utility
CEDS
information
next
grid
help
Yes
one
now
use
push
See
work
trusted
truth
will
share
risk
DOD
get
response
lot
take
cost
just
free
right
cyber
open
way
back
device
OSINT
want
many
info
safety
E-ISAC
group
used