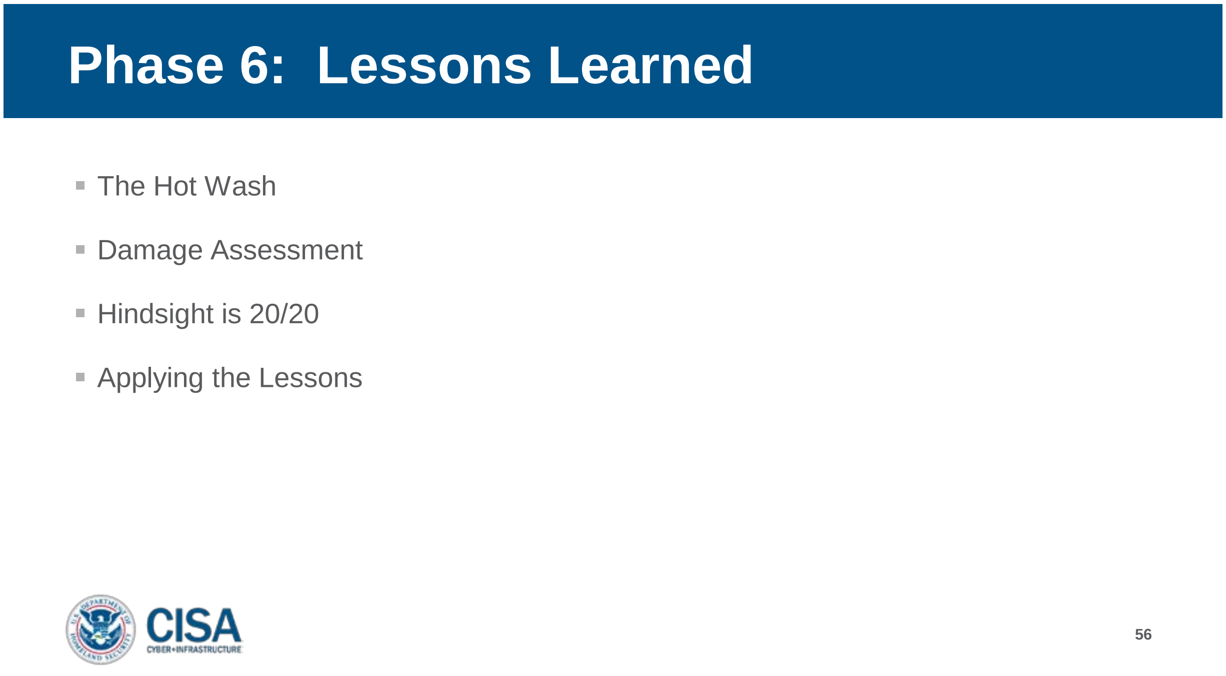
Incident Response Phase 6 of 6 – Lessons Learned

Table of Contents

Phase 6: Lessons Learned



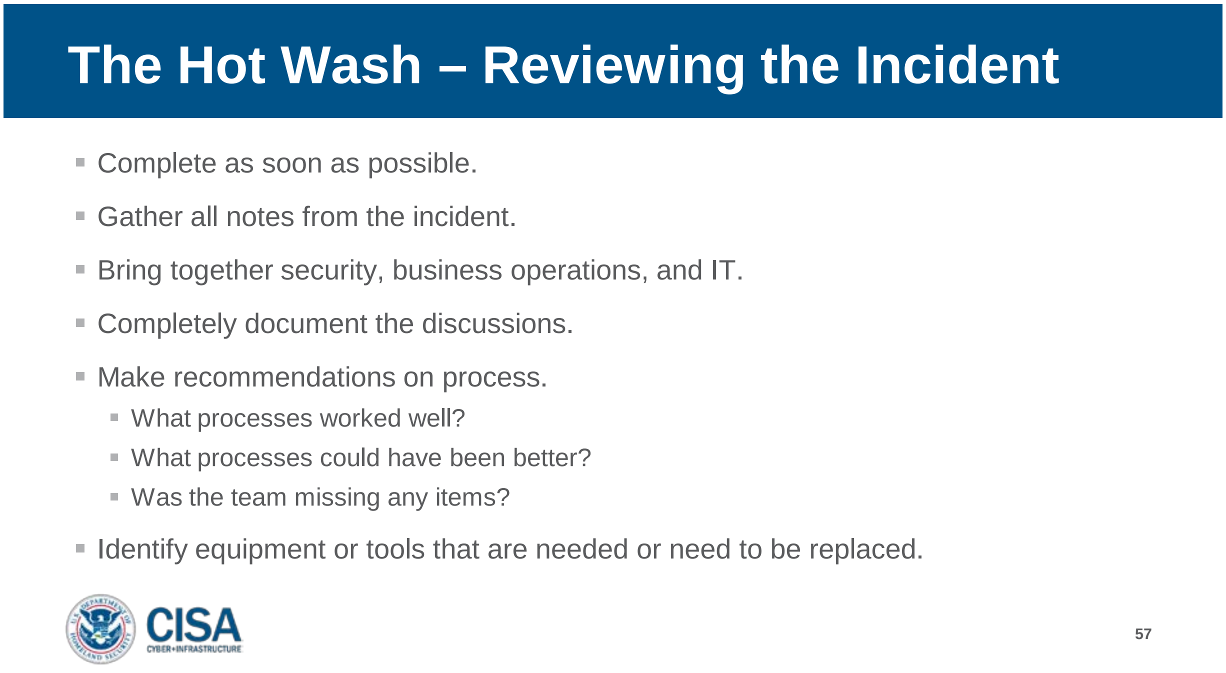
Phase 6: Lessons Learned

- The Hot Wash
- Damage Assessment
- Hindsight is 20/20
- Applying the Lessons

56

**056 Instructor: Treat all incidents as lesson learned opportunities. Here are some things we're going to talk about so that way we can grow in maturity as a security organization.

The Hot Wash – Reviewing the Incident

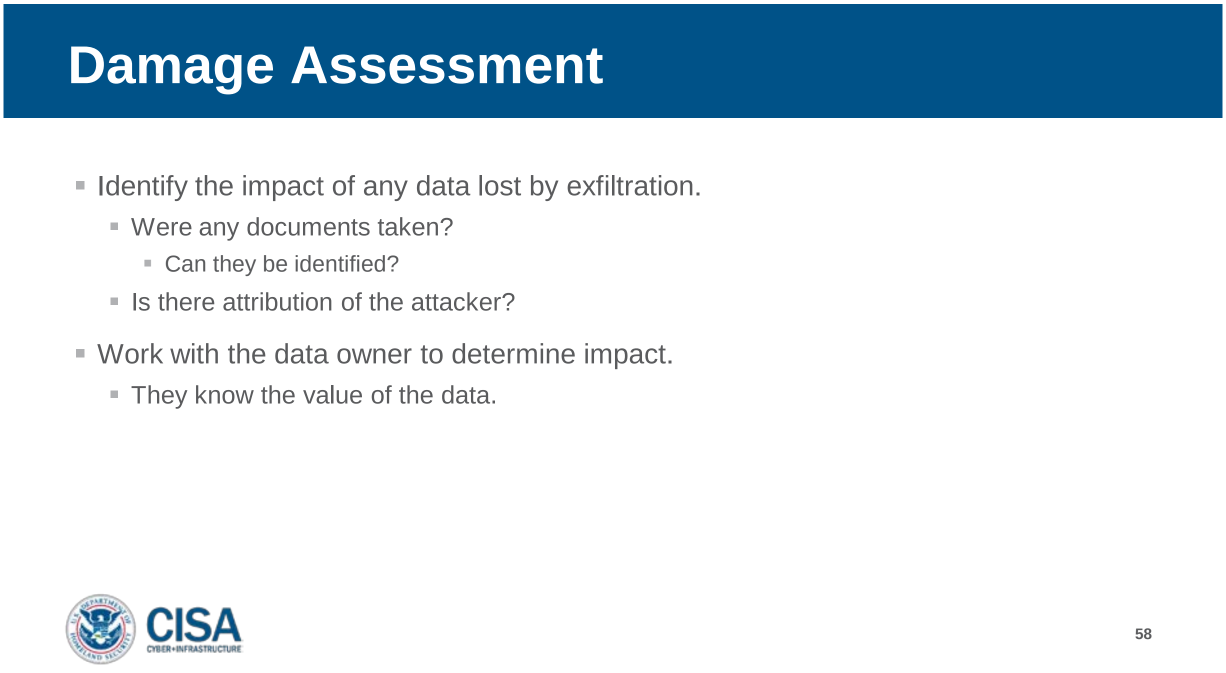


The Hot Wash – Reviewing the Incident

- Complete as soon as possible.
- Gather all notes from the incident.
- Bring together security, business operations, and IT.
- Completely document the discussions.
- Make recommendations on process.
  - What processes worked well?
  - What processes could have been better?
  - Was the team missing any items?
- Identify equipment or tools that are needed or need to be replaced.

**057 A hot wash, this is nothing more than review of the incident. And typically, what you want to do is have a hot wash as soon as the event is cleared up. The reason being is there's going to be a knowledge decay. People are going to forget what specifically happened. So, make sure you gather all the documentation that you have, all the notes of what happened. Make people write it down. Make them write down their experience, and that way, as you get together as a group, you can have very interactive discussions to find out who did what. Did they do it well? Can they do things better? And if they're missing anything, this may be an opportunity for some training, so that way we can grow together as an organization and mature in our security program.

Damage Assessment



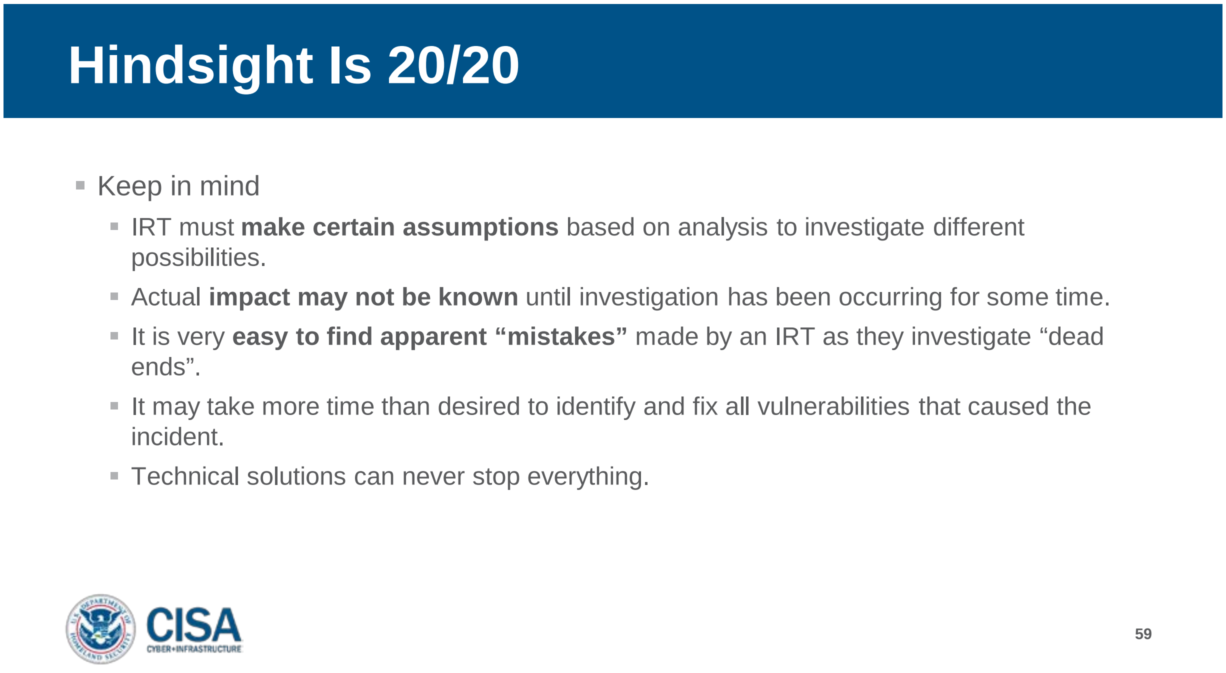
Damage Assessment

- Identify the impact of any data lost by exfiltration.
  - Were any documents taken?
    - Can they be identified?
  - Is there attribution of the attacker?
- Work with the data owner to determine impact.
  - They know the value of the data.

58

**058 It may also come down to understanding the extent of impact on an enterprise. This is harder than it sounds. Technically, if you've lost some intellectual property, it could be very challenging to understand how much value can be assigned to that intellectual property, especially if it's for a product that's not even in the wild yet, and you really have trouble assigning value even knowing that there could be potential future customers that really don't even know that it exists yet. This can be a real challenge. So, it's a good idea to work with data owners to understand exactly what you have and understand how they value that product and strategically how they want to leverage it in the future.

Hindsight Is 20/20



Hindsight Is 20/20

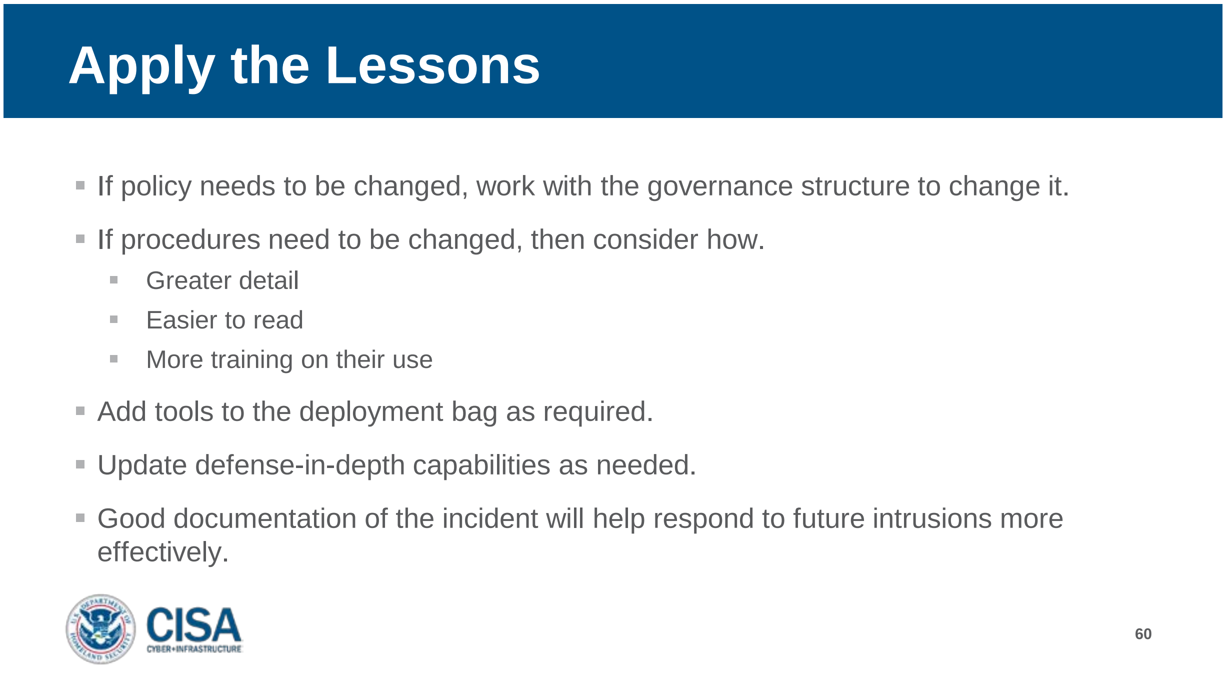
- Keep in mind
  - IRT must **make certain assumptions** based on analysis to investigate different possibilities.
  - Actual **impact may not be known** until investigation has been occurring for some time.
  - It is very **easy to find apparent “mistakes”** made by an IRT as they investigate “dead ends”.
  - It may take more time than desired to identify and fix all vulnerabilities that caused the incident.
  - Technical solutions can never stop everything.

59

**059 Hindsight's always 20/20. So, you have to keep in mind that the incident response team, it has to make certain assumptions so that way they're actually going to make critical business decisions correctly the first time. Sometimes, they're going with their gut. You also have to know that sometimes the impact may not be known to its fullest extent until even months down the road or even farther.

There are going to be mistakes. You want to be careful not to be so critical of your incident response team, especially if they run into a lot of dead ends. Be patient. Some of this actually takes time. Technical solutions can't necessarily stop everything, and people are critical. So, make sure those people are supported as best as possible to get the job done well.

Apply the Lessons



Apply the Lessons

- If policy needs to be changed, work with the governance structure to change it.
- If procedures need to be changed, then consider how.
  - Greater detail
  - Easier to read
  - More training on their use
- Add tools to the deployment bag as required.
- Update defense-in-depth capabilities as needed.
- Good documentation of the incident will help respond to future intrusions more effectively.

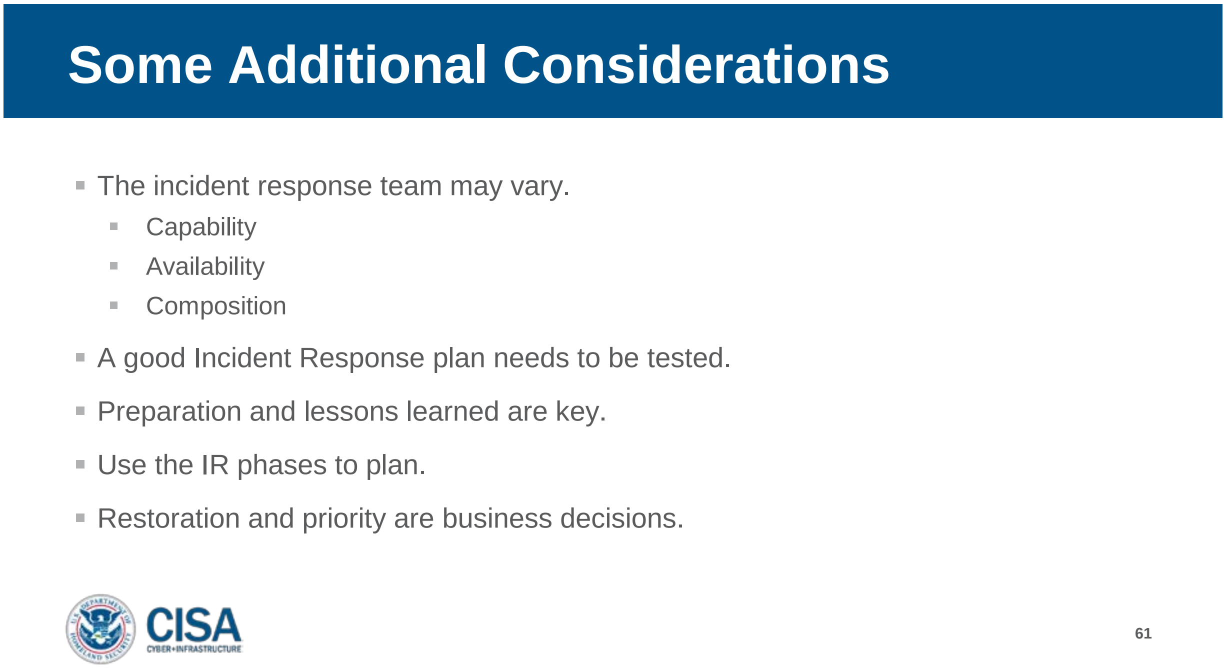
CISA
CYBER+INFRASTRUCTURE

60

**060 And by the way, when you've done these lessons learned, don't put it in a drawer somewhere. Don't let it sit around and collect dust. Be sure to educate your organization. And you can get help with your governance structure. Make sure you work with them, so that way they're advocating for correct actions to be taken.

You could take this as a learning opportunity to review your existing policies and procedures. Is there enough detail in them? Were they easy enough to read and understand by the people who had to execute them? Is there more training necessary in the organization? And maybe it's the idea too that it's not actually the incident response team that needed the training. Maybe it's the users. So, you have to think about the stakeholders that need to have this type training too. Maybe you need more tools in your deployment bag or maybe even new applications in your security stack. Either way, you want to keep that clear defense-in-depth strategy going, and you have to understand if you need to add more layers to keep the threats out. In all cases, make sure you document it

Some Additional Considerations



Some Additional Considerations

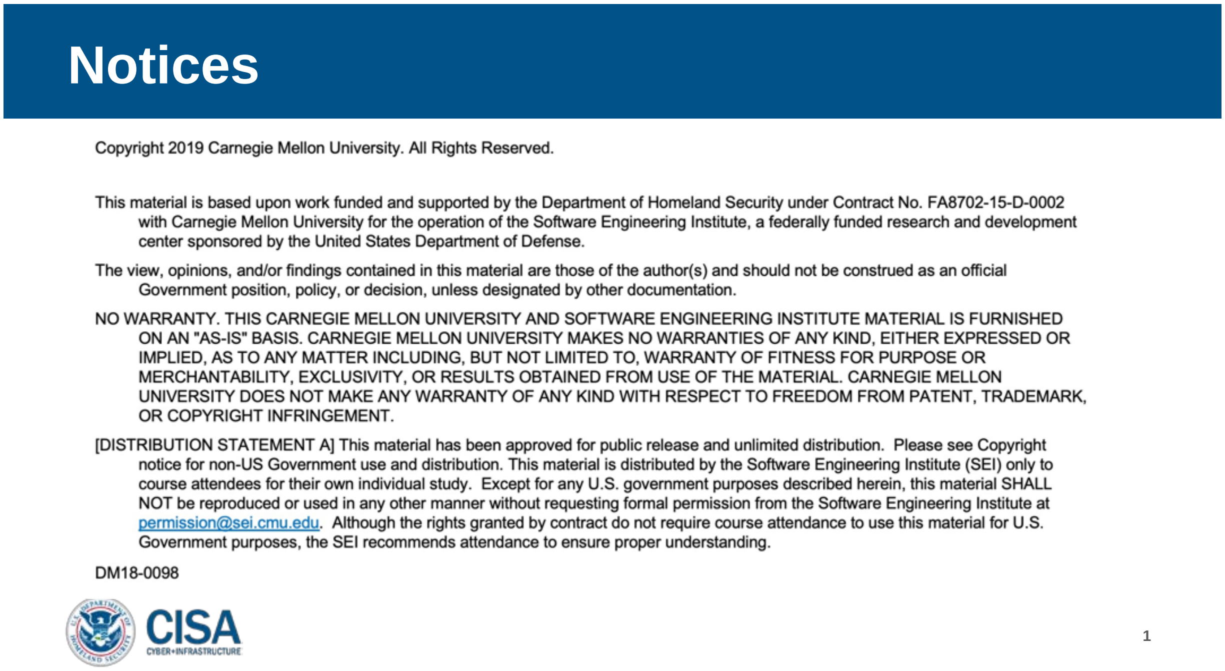
- The incident response team may vary.
  - Capability
  - Availability
  - Composition
- A good Incident Response plan needs to be tested.
- Preparation and lessons learned are key.
- Use the IR phases to plan.
- Restoration and priority are business decisions.

CISA
CYBER+INFRASTRUCTURE
61

**061 Some last things to think about here, too. For your incident response team, you know that you want to keep them as diverse a crowd as possible. And I'm talking about their capabilities, their skills, and maybe even their availability at times. Not all viruses hit at ten o'clock in the morning or right after lunch when it's convenient. It's going to be late at night. So, you've got to remember that this team is going to need rest as well. You're going to want to have additional employees standing by who can supplement the team in those darkest days when things are just not going well and you're going to need extra help.

You need to test that team too. Make sure people know what their responsibilities are. Make sure that they're prepared, and they're trained properly to conduct a proper incident response plan. Remember, restoration comes down to appropriate and proper business decisions. It's not just teaching people about bits and bytes. You have to be sure that your incident response team understands the organizational goals and objectives, so that way they make the right response.

Notices



Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM18-0098